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.
11/325,719	05/21/2013	8447695	IN920050028US1	7235

26502 7590 05/01/2013

IBM CORPORATION
IPLAW SHCB/256-3
1701 NORTH STREET
ENDICOTT, NY 13760

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 2021 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):

Vijil Enara Chenthamarakshan, Palghat, INDIA;

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.

1 fw
$

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)

30449 7590 01/14/2013
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

OPAP IAP11 APR 1 1 2013 PATENT & TRADEMARK OFFICE

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

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/325,719	01/05/2006	Vijil Enara Chenthamarakshan	IN920050028US1	7235

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	04/15/2013

04/12/2013 AWONDAF2 00000042 090457 11325719

EXAMINER	ART UNIT	CLASS-SUBCLASS
NILFOROUSH, MOHAMMAD A	3685	705-050000

01 FC:1501 1780.00 DA
02 FC:1504 300.00 DA

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 Schmeiser, Olsen & Watts;
2 John Pivnichny
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: International Business Machines Corporation
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Armonk, NY

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 090457 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above) (IBM)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

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

Authorized Signature Jack P. Friedman Date 02/22/2013

Typed or printed name Jack P. Friedman Registration No. 44,688

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.

OPAP
APR 1 1 2013
IAP11
PATENT & TRADEMARK OFFICE

PTO/SB/122 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
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.

CHANGE OF CORRESPONDENCE ADDRESS
Application

Address to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/325,719
Filing Date	2006-01-05
First Named Inventor	VIJIL ENARA CHENTHAMARAKSHAN
Art Unit	3685
Examiner Name	NILFOROUSH, MOHAMMAD A.
Attorney Docket Number	IN920050028US1

Please change the Correspondence Address for the above-identified patent application to:

☑ The address associated with Customer Number: 26,502

OR

☐ Firm or Individual Name

Address

City | State | Zip

Country

Telephone | Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

☐ Applicant/Inventor

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

☑ Attorney or agent of record. Registration Number 44,688.

☐ Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number_____.

Signature: Jack P. Friedman

Typed or Printed Name: Jack P. Friedman

Date: 02/22/2013 | Telephone: 518 220-1850

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 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 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.

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	11/325,719	CHENTHAMARAKSHAN, VIJIL ENARA	
	Examiner	Art Unit	
	Mohammad A. Nilforoush	3685	

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

(1) *Mohammad A. Nilforoush*. (3)_____.

(2) *Jack P. Friedman (Reg. No. 44,688)*. (4)_____.

Date of Interview: *12/4 & 12/31, 2012*.

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: *1, 16, and 26*.

Identification of prior art discussed: _____.

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...)

Applicant's representative, Mr. Jack P. Friedman (Reg. No. 44,688), authorized the amendments reflected in the Examiner's Amendment.

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

/M. A. N./ Examiner, Art Unit 3685	

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 4
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

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

30449 7590 01/14/2013
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER
NILFOROUSH, MOHAMMAD A

ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 01/14/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/325,719	01/05/2006	Vijil Enara Chenthamarakshan	IN920050028US1	7235

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	04/15/2013

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 SMALL ENTITY status shown above.

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

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

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

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

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

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

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

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

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 5
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

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)

30449 7590 01/14/2013
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/325,719	01/05/2006	Vijil Enara Chenthamarakshan	IN920050028US1	7235

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1770	$300	$0	$2070	04/15/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
NILFOROUSH, MOHAMMAD A	3685	705-050000

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

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

1 _____
2 _____
3 _____

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

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

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

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

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

Security First Innovations, LLC, Exhibit 2014
Page 1 of 6
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

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.
11/325,719	01/05/2006	Vijil Enara Chenthamarakshan	IN920050028US1	7235

30449 7590 01/14/2013
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER
NILFOROUSH, MOHAMMAD A

ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 01/14/2013

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 1722 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 1722 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.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 7
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

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.

Notice of Allowability	Application No.	Applicant(s)	
	11/325,719	CHENTHAMARAKSHAN, VIJIL ENARA	
	Examiner	**Art Unit**	
	Mohammad A. Nilforoush	3685	

-- 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 *Interview on 12/4/2012 with Mr. Jack P. Friedman (Reg. No. 44,688)*.

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 *1-12, 14-22, 24-32 and 34-35*. 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).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

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

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)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 1/5/2006
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/4/2012* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/M. A. N./
Examiner, Art Unit 3685

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 9
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

EXAMINER'S AMENDMENT

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 telephone interviews with Mr. Jack P. Friedman (Reg. No 44,688) on 12/4/2012 and 12/31/2012.

The application has been amended as follows:

Please amend claims 1, 16, and 26 in the set of claims filed 1/28/2010 as follows:

1. A method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising a processor, the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises:

said processor via execution of the feedback module, establishing a secret key k(0), ~~a~~ said feedback module ~~and~~ sending the key k(0) to the vendor ~~sharing the key k(0)~~, and communicating the key k(0) to a user of the software, ~~wherein the user is external to the end user machine~~;

said processor via execution of the feedback module, establishing a secret key n(0), the feedback module ~~and~~ sending the key n(0) to the vendor ~~sharing the key n(0)~~, and not communicating the key n(0) to the user;

~~a~~ said processor, via execution of ~~a~~ the feedback module, generating an identification tag FE(0) ~~that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database~~;

said processor, via execution of the feedback module, generating a secret key s(0) and communicating the generated key s(0) to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) where ~~such that~~ E_{k0} = E(k(0),FE(0));

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) where ~~such that~~ H_{n0} = Hash(n(0) || Ek0);

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) where ~~such that~~ H_{s0} = Hash(s(0) || Ek0);

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.[[,]]

~~wherein~~

16. A computer program product, comprising a non-volatile computer readable storage medium having a computer readable program code stored therein, ~~execution of said computer readable program code causing a processor to implement~~ said computer readable program code, upon being executed by a processor, performs a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising the processor, the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises:

said processor via execution of the feedback module, establishing a secret key k(0), ~~a~~ said feedback module ~~and~~ sending the key k(0) to the vendor ~~sharing the key k(0)~~, and communicating the key k(0) to a user of the software, ~~wherein the user is external to the end user machine~~;

said processor via execution of the feedback module, establishing a secret key n(0), the feedback module ~~and~~ sending the key n(0) to the vendor ~~sharing the key n(0)~~, and not communicating the key n(0) to the user;

said processor, via execution of ~~a~~ the feedback module, generating an identification tag FE(0) ~~that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database~~;

said processor, via execution of the feedback module, generating a secret key s(0) and communicating the generated key s(0) to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) where ~~such that~~ E_{k0}= E(k(0),FE(0));

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) where ~~such that~~ H_{n0} = Hash(n(0) || E_{k0});

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) where ~~such that~~ H_{s0} = Hash(s(0) || E_{k0});

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

26. (Currently amended) A process for deploying (or integrating) computing infrastructure, said process comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of performing a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising a processor, the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises:

said processor via execution of the feedback module, establishing a secret key k(0), ~~a~~ said feedback module ~~and~~ sending the key k(0) to the vendor ~~sharing the key k(0)~~, and communicating the key k(0) to a user of the software, ~~wherein the user is external to the end user machine~~;

said processor via execution of the feedback module, establishing a secret key n(0), the feedback module ~~and~~ sending the key n(0) to the vendor ~~sharing the key n(0)~~, and not communicating the key n(0) to the user;

~~a~~ said processor, via execution of ~~a~~ the feedback module, generating an identification tag FE(0) ~~that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database~~;

said processor, via execution of the feedback module, generating a secret key s(0) and communicating the generated key s(0) to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) where ~~such that~~ E_{k0} = E(k(0),FE(0));

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) where ~~such that~~ H_{n0} = Hash(n(0) || Ek0);

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) where ~~such that~~ H_{s0} = Hash(s(0) || Ek0);

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

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

The present invention is directed to method of processing feedback entries received from software. The feedback entry is encrypted with a secret key k(0), and two hashes are generated based on the encrypted feedback entry. The first hash is generated by concatenating a key n(0), that is shared between the feedback module and the vendor, to the encrypted feedback entry and hashing the result. This hash is sent to the vendor along with the encrypted feedback entry. The second hash is generated by the feedback module generating a key s(0) that is shared with the user, concatenating s(0) to the encrypted feedback entry, and hashing the result. This hash is stored in a database on the end user machine along with the encrypted feedback entry.

The closest prior art of Orisini (US 2006/0177061) discloses a trust engine receiving a hash of a contract, signs it with the user's private key, and sends this signed hash to the vendor (Orisini **¶¶ 276-277**). Orisini also discloses the trust engine preparing a hash of the contract with the vendor's private key and forwarding this to the user (Orisini **¶¶ 278**). Elgamal also discloses a client and a server establishing session keys and communicating with each other using the session keys (Elgamal **2:5-10**; **7:41-51**; **23:9-19**; **27:51-54**; **33:1-13**).

However, with regard to claims 1, 16, and 26, the prior art does not disclose, singly or in combination, that the data is encrypted by the feedback module, or said

processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that H_{n0} = Hash(n(0) || E_{k0}); said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that H_{s0} = Hash(s(0) || E_{k0}); said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

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."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad A. Nilforoush whose telephone number is (571)270-5298. The examiner can normally be reached on M-F 10am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt can be reached on (571)270-6709. 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.

/M. A. N./
Examiner, Art Unit 3685

/CALVIN L HEWITT II/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 11/325,719	Applicant(s)/Patent Under Reexamination CHENTHAMARAKSHAN, VIJIL	
	Examiner Mohammad A. Nilforoush	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0177061 A1	08-2006	Orsini et al.	380/268
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	MOHAMMAD A NILFOROUSH	3685

ORIGINAL		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
705	50	G	0	6	F	21 / 00 (2006.01.01)						

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
705	64				
380	278				

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

/MOHAMMAD A NILFOROUSH/ Examiner.Art Unit 3685	12/4/12	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	32	
/CALVIN L HEWITT II/ Supervisory Patent Examiner.Art Unit 3685	01/04/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	4

INFORMATION DISCLOSURE STATEMENT PURSUANT TO 37 C.F.R. §§1.97-1.99

PATENT APPLICATION

Applicant(s): Vijil Enara Chenthamarakshan Docket No.: IN920050028US1

FOR: **SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE**

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

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56 and pursuant to 37 C.F.R. §§1.97-1.99, Applicant(s) hereby notifies the U.S. Patent and Trademark Office of the documents listed on the attached Form PTO-1449. Applicant respectfully submits that all pending claims are patentable over the foregoing references, alone or in combination. The Examiner is requested to initial the enclosed Form PTO-1449 and return a copy thereof to the undersigned.

The submission of the listed documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant reserves the right to dispute any of the listed documents as prior art during examination. Further, Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application. Furthermore, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made or that no other material information may exist. This Information Disclosure Statement is being filed within three months of the filing date of the captioned patent application, and therefore no certification under 37 C.F.R. §1.97(e) or fee under 37 C.F.R. §1.17(p) is required.

Respectfully submitted,

Dated: 12/01/2005

By Jack P. Friedman
Jack P. Friedman
Reg. No. 44,688

Enclosures: PTO-1449

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.N./

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	ATTY DOCKET NO. IN920050028US1	APPLICATION NO.
	APPLICANT(S) Vijil E. Chenthamarakshan	
	FILING DATE	GROUP ART UNIT

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		6,901,347	05/31/2005	Murray, *et al.*			
		6,842,752	01/11/2005	Itabashi, *et al.*			

U.S. PATENT APPLICATION PUBLICATIONS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2004/0210458	10/21/2004	Evans, *et al.*			
		2004/0167859	08/26/2004	Mirabella			
		2004/0139315	07/15/2004	Tokutani, *et al.*			
		2004/0034794	02/19/2004	Mayer, *et al.*			

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.N./

Security First Innovations, LLC, Exhibit 2014 Page 2014 - 21
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	ATTY DOCKET NO. IN920050028US1	APPLICATION NO.
	Vijil E. Chenthamarakshan	
	FILING	GROUP ART

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

U.S. PATENT APPLICATION PUBLICATIONS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2003/0133464	07/17/2003	Marejka, *et al.*			

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

EXAMINER	DATE CONSIDERED
/Mohammad Nilforoush/	03/27/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.N./

Security First Innovations, LLC Exhibit 2014 Page 2014 - 22
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S152	1067	(generat$3 calculat$3 produc$3) with (hash hmac MAC signature) with ((secret password key) near (user client customer consumer))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:33
S151	436	(generat$3 calculat$3 produc$3) with (hash hmac MAC signature) with ((secret password key) near (user client customer consumer))	USPAT; USOCR	OR	ON	2012/08/24 15:33
S154	44	S153 and (generat$3 calculat$3 produc$3) near3 ((secret password key) near (vendor server merchant provider distributor developer source))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:34
S153	69	S152 and (generat$3 calculat$3 produc$3) with (hash hmac MAC signature) with ((secret password key) near (vendor server merchant provider distributor developer source))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:34
S157	69	S156 and (generat$3 calculat$3 produc$3) with (hash hmac MAC signature) with ((secret password key) near (vendor server merchant provider distributor developer source))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:35
S156	1271	(creat$ generat$3 calculat$3 produc$3) with (hash hmac MAC signature) with ((secret password key) near (user client customer consumer))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:35
S155	44	S153 and (creat$3 generat$3 calculat$3 produc$3) near3 ((secret password key) near (vendor server merchant provider distributor developer source))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:35
S160	52	S159 and (creat$3 generat$3 calculat$3 produc$3) near3 ((secret password key) near (vendor server merchant provider distributor developer source))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:36
S159	81	S156 and (creat$3 generat$3 calculat$3 produc$3) with (hash hmac MAC signature) with ((secret password key) near (vendor server merchant provider distributor developer source))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:36
S158	44	S157 and (generat$3 calculat$3 produc$3) near3 ((secret password key) near (vendor server merchant provider distributor developer source))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 15:36
S161	17	S160 and (creat$3 generat$3 calculat$3 produc$3) near3 ((secret password key) near (user client customer consumer))	USPAT; USOCR	OR	ON	2012/08/24 15:37
S168	343	secret adj prefix	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 16:54

S169	1	("8250372").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/08/24 17:28
S175	1	WO-0124012-$.did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/08/24 17:33
S176	2	(("5724424") or ("6049785")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/08/24 18:02
S177	92	(generat$3 calculat$3 determin$3 produc$3) with (unique near2 (HMAC signature MAC (authentication adj (code value))) near2 (party side user))	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 18:11
S178	1456	(generat$3 calculat$3 determin$3 produc$3) with ((two multiple several different) near2 (HMAC signature MAC (authentication adj (code value)))) with (data message file content)	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 18:24
S179	17	S178 same (secret key password) near2 (user client consumer customer)	US-PGPUB; USPAT; USOCR	OR	ON	2012/08/24 18:49
S180	4	("2005/0182932").URPN.	USPAT	OR	ON	2012/09/17 13:53
S181	1	"5794207".pn.	USPAT	OR	ON	2012/09/17 14:15
S196	1112	S195 and @ay<"2006"	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 14:00
S195	1887	S194 and (prefix)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 14:00
S194	21390	(snmp (simple adj network adj management))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 14:00
S197	350	S196 and (central third) adj2 (server party controller authority)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 14:01
S198	0	S194 and (secret adj prefix)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 14:02
S200	19	("5220501" | "5809144" | "5901229" | "5909492" | "6029150").PN. OR ("6742125").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 15:33
S199	1	("6742125").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/09/19 15:33
S201	349	(send$3 transmit$4) with (copy duplicate) with (customer client user purchaser buyer) with (seller merchant retailer offer?r vendor)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 15:49
S203	69	S201 and (MAC HMAC hash signature checksum (authentication adj code) (verification adj value)) with (different unique separate)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 15:50

S202	0	S201 same (MAC HMAC hash signature checksum (authentication adj code) (verification adj value)) with (different unique separate)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 15:50
S204	4	(central third authority broker server) with (send$3 transmit$4) with (copy duplicate) with ((other both every all) near (party))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 15:53
S205	1	("2005/0182684").URPN.	USPAT	OR	ON	2012/09/19 16:32
S206	7	("20020198848" | "20040073688" | "20050182684" | "20060129502" | "20070150744" | "20080234052" | "20090283589").PN. OR ("7725403").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 16:53
S208	21	((seller merchant retailer offer?r vendor) near2 (copy duplicate)) with ((seller merchant retailer offer?r vendor) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:45
S207	529	((customer client user purchaser buyer) near2 (copy duplicate)) with ((customer client user purchaser buyer) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:45
S209	2	S207 and S208	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:46
S210	529	((customer client user purchaser buyer (party near ("A" first))) near2 (copy duplicate)) with ((customer client user purchaser buyer (party near ("A" first))) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:48
S211	21	(((party near ("A" second other another)) seller merchant retailer offer?r vendor) near2 (copy duplicate)) with (((party near ("A" second other another)) seller merchant retailer offer?r vendor) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:49
S212	1363	((customer client user purchaser buyer (party near ("A" first))) near2 (version copy duplicate)) same ((customer client user purchaser buyer (party near ("A" first))) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:50
S213	45	(((party near ("A" second other another)) seller merchant retailer offer?r vendor) near2 (version copy duplicate)) same (((party near ("A" second other another)) seller merchant retailer offer?r vendor) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:51
S214	3	S212 and S213	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/19 20:53
S215	7	("20030133464" | "20040034794" | "20040139315" | "20040167859" | "20040210458" | "6842752" | "6901347").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 16:06
S216	27	(creat$3 generat$3) with verifiable with log	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 16:27
S217	58	(creat$3 generat$3) with (verifiable	US-PGPUB;	OR	ON	2012/09/25

		authenticatable) with (log report)	USPAT; USOCR			16:38
S218	0	S217 and independently near2 (authenticat$3 verif$7) with (report log)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 16:50
S219	302	independently near2 (authenticat$3 verif$7) with (report log contract receipt message copy)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 16:51
S220	19	independently near2 (authenticat$3 verif$7) with (report log contract receipt message copy) with (parties)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 16:56
S222	3538	S221 same (user client customer consumer buyer enduser) near3 (key secret)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 16:59
S221	53016	(signature sign$3 hash$3) with (user client customer consumer buyer enduser) with (message copy contract report log receipt)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 16:59
S223	622	S222 and ((signature sign$3 hash$3) with (vend?r server merchant retailer seller provider offer?r distributor) with (message copy contract report log receipt)) same ((vend?r server merchant retailer seller provider offer?r distributor) near3 (key secret))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 17:01
S224	0	separ?tely near2 (authenticat$3 verif$7) with (report log contract receipt message copy) with (parties)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 17:05
S225	0	S217 and separ?tely near2 (authenticat$3 verif$7) with (report log)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/25 17:06
S226	59	("2006/0177061").URPN.	USPAT	OR	ON	2012/09/26 19:56
S227	162	("20010001876" | "20010051902" | "20020010679" | "20020032663" | "20020035664" | "20020046359" | "20020071566" | "20020091640" | "20020129235" | "20020162047" | "20020172358" | "20030051054" | "20030051159" | "20030058274" | "20030070077" | "20030167408" | "20040049687" | "20040111608" | "20040122863" | "20040123863" | "20060177061" | "20060184764" | "20060282681" | "20060288425" | "20060294378" | "20070006326" | "20070101436" | "20070160198" | "20070192586" | "20080137857" | "20080170693" | "20080183975" | "20080183992" | "20080199003" | "20080244277" | "20090077379" | "20090177894" | "20090254750" | "20100150341" | "20100153670" | "20100153703" | "20100154053" | "20100299313" | "20110179271" | "20110179287" | "4453074" | "4924513" | "4932057" | "5010572" | "5016274" | "5051745" | "5150407" | "5163096" | "5268963" | "5375244" | "5386104" | "5485474" | "5524073" | "5615269" |	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/26 19:59

		"5642508" | "5666414" | "5666416" | "5682425" | "5703907" | "5717758" | "5748735" | "5761306" | "5768382" | "5768519" | "5790677" | "5823948" | "5903652" | "5903882" | "5910987" | "5915019" | "5917913" | "5940507" | "5960083" | "5966444" | "5966448" | "5974144" | "5982322" | "5987232" | "5991414" | "5995630" | "6009177" | "6023508" | "6026163" | "6061790" | "6073237" | "6092201" | "6094485" | "6134550" | "6192472" | "6229894" | "6240183" | "6240187" | "6256737" | "6260125" | "6266413" | "6289455" | "6289509" | "6292568" | "6292782" | "6301659" | "6307940" | "6314409" | "6324650" | "6336186" | "6345101").PN. OR ("6345314" | "6356941" | "6363425" | "6385318" | "6386451" | "6411716" | "6424718" | "6438690" | "6446204" | "6449730" | "6453416" | "6483921" | "6553493" | "6615347" | "6625734" | "6631201" | "6684330" | "6687375" | "6789198" | "6852988" | "6856383" | "6952684" | "6959383" | "6965993" | "6978367" | "7003531" | "7050580" | "7050583" | "7069451" | "7096494" | "7117365" | "7133845" | "7140044" | "7187771" | "7203871" | "7218736" | "7225158" | "7313825" | "7322047" | "7337320" | "7349539" | "7349987" | "7391865" | "7546427" | "7552482" | "7577689" | "7627125" | "7649992" | "7669051" | "7721344" | "7869597" | "8009830").PN.				
S229	11	signature with (each every) adj party	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/26 20:17
S228	9	individualized near2 ((hash authentication verification) near (value))	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/26 20:17
S231	15	((((hash authentication verification) near (value)))) with (each every) near2 (copy version duplicate)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/26 20:19
S230	0	(unique near2 (((hash authentication verification) near (value)))) with (each every) near2 (copy version duplicate)	US-PGPUB; USPAT; USOCR	OR	ON	2012/09/26 20:19
S234	1	"20020042782"	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 16:32
S233	2	"20040054606"	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 16:32
S232	0	"10777717"	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 16:32
S235	4	(("20040054606") or ("20020042782") or ("7051364") or ("20020157004")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/03 16:33
S236	9340	((customer client user purchaser buyer (first adj party) (party adj A))) with	US-PGPUB; USPAT;	OR	ON	2012/10/03 18:29

		(verify$3 authenticat$3 verification) with ((customer client user purchaser buyer (first adj party) (party adj A)) near2 (key))	USOCR			
S237	12336	((customer client user purchaser buyer (first adj party) (party adj A))) with (verify$3 authenticat$3 verification) with ((customer client user purchaser buyer (first adj party) (party adj A) private secret) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 18:32
S240	485	S237 and (((party near ("B" second other another)) seller merchant retailer offer?r vendor)) with (verify$3 authenticat$3 verification) with (((party near ("B" second other another)) seller merchant retailer offer?r vendor secret private) near2 (key))	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 18:33
S243	300	S241 and (customer client user purchaser buyer (first adj party) (party adj A)) with (hash signature hmac ((verification authentication) adj value))	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 18:35
S241	329	S240 and (((party near ("B" second other another)) seller merchant retailer offer?r vendor)) with (hash signature hmac ((verification authentication) adj value))	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 18:35
S245	177	S244 and (customer client user purchaser buyer (first adj party) (party adj A)) near2 (hash signature hmac ((verification authentication) adj value))	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 18:36
S244	230	S240 and (((party near ("B" second other another)) seller merchant retailer offer?r vendor)) near2 (hash signature hmac ((verification authentication) adj value))	US-PGPUB; USPAT; USOCR	OR	ON	2012/10/03 18:36
S246	1	("6163841").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/17 18:39
S247	1	("20020164026").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/10/17 18:57

12/4/2012 7:26:50 PM
C:\ Users\ mnilforoush\ Documents\ EAST\ Workspaces\ Mohammad\ 11325719.wsp

Business Methods Intranet

BUSINESS-CRYPTOGRAPHY
Dialog Toolkit Interface

POWERED BY Dialog LOGOFF

Search results: 0 titles

Search Report

Database Name	Database Number
ABI/INFORM	15
COMPUTER DATABASE	275
NEW PRODUCT ANNMNT	621
NEWSLETTER DB	636
TRADE&INDUSTRY	148
PROMT (90-PRESENT)	16
PROMT (1972-1989)	160

Set	Description
S1	PY=((1970:2006))
S2	S1 (((customer OR client OR user OR purchaser OR buyer OR (first (w) party) OR (party (w) A))) (s) (verify? OR authenticat? OR verification) (s) ((customer OR client OR user OR purchaserOR buyer (first (w) party) OR (party (w) A) OR private OR secret) (2n) (key))) AND ((((party (n) ("B" OR second OR other OR another)) seller OR merchant OR retailer OR offerer OR offeror OR vendor)) (s) (verify$3 OR authenticat$3 OR verification) (s) (((party (n) ("B" OR second OR other another)) seller OR merchant OR retailer OR offer?r OR vendor OR secret OR private) (2n) (key)))
S3	SORT /ALL/pd,a

Help Tips for 'Zero Records' - How To Get More Records

- Don't over-specify: use only the search options you really need -- leave the others blank.
- Exclude "implied concepts": leave out words like 'research' or 'effects.'
- Use more wildcards to search different word endings: use COMPUTER? in place of COMPUTER.
- Check the format of your entry. Follow the Search Tips examples shown on the search page.
- Check for misspelled words.
- Check that you are using parentheses correctly when you combine words with AND, OR, NOT.

For more tips on searching, see the Help page.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	MOHAMMAD NILFOROUSH	3685

✓	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	03/17/2009	12/04/2012							
	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	✓	=							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	Mohammad A Nilforoush	3685

SEARCHED

Class	Subclass	Date	Examiner
705	all	1/8/2013	/M. A. N./

SEARCH NOTES

Search Notes	Date	Examiner
Keyword search (see EAST search history)	3/27/2009	/M. A. N./
Search of relevant references (see EAST search history)	3/27/2009	/M. A. N./
Citation search of relevant references (see EAST search history)	3/27/2009	/M. A. N./
Inventor name search (see EAST search history)	3/27/2009	/M. A. N./
Updated Search (see EAST search history)	10/28/2009	/M. A. N./
Updated Search (see EAST search history)	12/4/2012	/M. A. N./
NPL Search (see DIALOG search history)	12/4/2012	/M. A. N./

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
705	all	1/8/2013	/M. A. N./

/M. A. N./ Examiner.Art Unit 3685	

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11325719	Filing Date	2006-01-05	Docket Number (if applicable)	IN920050028US1	Art Unit	3685
First Named Inventor	V. Chenthamarakshan			Examiner Name	Nilforoush, Mohammed A.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 090457

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature
☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Jack P. Friedman/	Date (YYYY-MM-DD)	2010-01-28
Name	Jack P. Friedman	Registration Number	44688

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 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.

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 the Freedom of Information Act requires disclosure of these records.

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 inspections 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:	11325719
Filing Date:	05-Jan-2006
Title of Invention:	System and method for processing feedback entries received from software
First Named Inventor/Applicant Name:	Vijil Enara Chenthamarakshan
Filer:	Jack P. Friedman/Kimberly Dwileski
Attorney Docket Number:	IN920050028US1

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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	1801	1	810	810
		Total in USD ($)		**810**

Electronic Acknowledgement Receipt

EFS ID:	6899804
Application Number:	11325719
International Application Number:	
Confirmation Number:	7235
Title of Invention:	System and method for processing feedback entries received from software
First Named Inventor/Applicant Name:	Vijil Enara Chenthamarakshan
Customer Number:	30449
Filer:	Jack P. Friedman/Kimberly Dwileski
Filer Authorized By:	Jack P. Friedman
Attorney Docket Number:	IN920050028US1
Receipt Date:	28-JAN-2010
Filing Date:	05-JAN-2006
Time Stamp:	14:05:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$810
RAM confirmation Number	304
Deposit Account	090457
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	IN920050028US1-preliminaryamendment.pdf	3197724 d1fd2fd309d7742b02a5d01542f06321efa49b72	no	38
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	IN920050028US1-RCE.pdf	919060 3d64f76cdc8b5ab6ce3a11e03779f15045dac72b	no	3
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	30520 6cdf5ed6e35919ef7c3221407a9b64bac4de5417	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4147304		

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Vijil Enara Chenthamarakshan

Group Art Unit: 3685 / Conf. # 7235

Application No.: 11/325,719

Examiner: Nilforoush, Mohammed A.

Filing Date: 01/05/2006

Docket No.: **IN920050028US1**

Title: SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

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

PRELIMINARY AMENDMENT

Sir:

Please enter the following preliminary amendment.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 40
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In the Claims:

Please cancel claims 13, 23, and 33. Please amend claims 1, 12, 16, 22, 26, and 32. The claims are as follows:

1. (Currently amended) A method for processing feedback entries received from software, said software provided by a vendor to an end user machine, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises:

establishing a secret key k(0), ~~that is shared between~~ a feedback module and the vendor sharing the key k(0), and communicating the key k(0) to a user of the software, wherein the user is external to the end user machine;

establishing a secret key n(0), ~~that is shared between~~ the feedback module and the vendor sharing the key n(0), ~~but~~ and not communicating the key n(0) to the user;

a processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database;

said processor, via execution of the feedback module, generating a secret key s(0) and communicating the generated key s(0) to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$;

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that $H_{n0} = Hash(n(0) \| E_{k0})$;

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 41
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that $H_{s0} = \text{Hash}(s(0) \| E_{k0})$;

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor, wherein

2. (Previously presented) The method of claim 1, said method comprising:

said processor, via execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database.

3. (Previously presented) The method of claim 2, said method comprising said processor, via execution of the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), …, FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, …, N comprising:

calculating parameters E_{ki}, H_{ni}, and H_{si} such that $E_{ki} = E(k(i), FE(i))$, $H_{ni} = \text{Hash}(n(i) \| E_{ki})$, and $H_{si} = \text{Hash}(s(i) \| E_{ki})$;

writing E_{ki}, H_{ni}, and H_{si} to the database;

said processor, via execution of the feedback module, generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 42
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

4. (Previously presented) The method of claim 3, said method comprising said processor, via execution of the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

5. (Original) The method of claim 4, wherein M=1.

6. (Original) The method of claim 4, wherein M>1.

7. (Original) A validation method for validating the N feedback entries resulting from performance of the method of claim 4, said validation method comprising verifying, by the vendor, an integrity of the N feedback entries received by the vendor as a result of said sending to the vendor: ((E_{ki}, H_{ni}), i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

8. (Previously presented) The validation method of claim 7, wherein said verifying comprises:

setting i = 0 and H(0) = n(0);

executing iterations i = 0, 1, …, N of a loop, wherein executing each iteration i of the loop comprises: setting H'_{ni} = Hash(H(i) || E_{ki}); determining that $H'_{ni} = H_{ni}$; and responsive to said determining that $H'_{ni} = H_{ni}$, setting H(i+1) = Hash(H(i)) and k(i+1) = Hash(k(i));

after said executing:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 43
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

decrypting E(k(N+1), n(N+1)) using key k(N+1) to infer n(N+1);

determining that n(N+1) = H(N+1); and

responsive to said determining that n(N+1) = H(N+1), ascertaining that the integrity of the N feedback entries received by the vendor has been verified.

9. (Previously presented) The validation method of claim 7, wherein the validation method further comprises, as performed by the vendor prior to said verifying:

calculating $H'_{n0} = \text{Hash}(n(0) \| E_{k0})$;

determining that $H'_{n0} = H_{n0}$; and

responsive to said determining that $H'_{n0} = H_{n0}$, decrypting E_{ko} to infer FE(0) and recording that the database is set.

10. (Original) A validation method for validating the N feedback entries resulting from performance of the method of claim 3, said validation method comprising verifying, by the user, an integrity of the N feedback entries in the database as a result of writing $((E_{ki}, H_{ni}, H_{si}), i= 1, \ldots, N)$ to the database.

11. (Previously presented) The validation method of claim 10, wherein said verifying comprises:

setting i = 0 and S(0) = s(0);

executing iterations i = 0, 1, …, N of a loop, wherein executing each iteration i of the loop comprises: setting $H'_{si} = \text{Hash}(S(i) \| E_{ki})$; determining that $H'_{si} = H_{si}$; and responsive to said determining that $H'_{si} = H_{si}$, setting S(i+1) = Hash(S(i));

after said executing:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 44
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

determining that S(N+1) = s(N+1); and

responsive to said determining that S(N+1) = s(N+1), ascertaining that the integrity of the N feedback entries in the database has been verified.

12. (Currently amended) The method of claim 1, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, wherein the feedback module is connected to both the application firewall and the database, wherein the software is connected to the feedback module, wherein the software is coupled to the application firewall via the feedback module, wherein the software is coupled to the database via the feedback module, and wherein the method further comprises:

said feedback module receiving the feedback entries from the software;

said feedback module writing, to the database, the feedback entries that the feedback module received from the software;

said application firewall preventing the software from accessing the communication network; and

said application firewall ~~permitting the feedback module to~~ controlling access of the communication network~~, said permitting being controlled by the application firewall~~ by the feedback module.

13. (Canceled)

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 45
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

14. (Original) The method of claim 12, wherein the communication network comprises the Internet.

15. (Original) The method of claim 1, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

16. (Currently amended) A computer program product, comprising a computer readable storage medium having a computer readable program code stored therein, execution of said computer readable program code causing a processor to implement a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises:

establishing a secret key k(0), ~~that is shared between~~ a feedback module and the vendor sharing the key k(0), and communicating the key k(0) to a user of the software, wherein the user is external to the end user machine;

establishing a secret key n(0), ~~that is shared between~~ the feedback module and the vendor sharing the key n(0), ~~but~~ and not communicating the key n(0) to the user;

said processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database;

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 46
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

said processor, via execution of the feedback module, generating a secret key s(0) and communicating the generated key s(0) to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$;

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that $H_{n0} = Hash(n(0) \| E_{k0})$;

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that $H_{s0} = Hash(s(0) \| E_{k0})$;

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

17. (Previously presented) The computer program product of claim 16, said method comprising:

said processor, via execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database.

18. (Previously presented) The computer program product of claim 17, said method comprising said processor, via execution of the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), …, FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, …, N comprising:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 47
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

calculating parameters E_{ki}, H_{ni}, and H_{si} such that $E_{ki} = E(k(i), FE(i))$, $H_{ni} = Hash(n(i) \| E_{ki})$, and $H_{si} = Hash(s(i) \| E_{ki})$;

writing E_{ki}, H_{ni}, and H_{si} to the database;

generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

19. (Previously presented) The computer program product of claim 18, said method comprising said processor, via execution of the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

20. (Original) The computer program product of claim 19, wherein M=1.

21. (Original) The computer program product of claim 19, wherein M>1.

22. (Currently amended) The computer program product of claim 16, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, <u>wherein the feedback module is connected to both the application firewall and the database, wherein the software is connected to the feedback module, wherein the software is coupled to the application</u>

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 48
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

firewall via the feedback module, wherein the software is coupled to the database via the feedback module, and wherein the method further comprises:

said feedback module receiving the feedback entries from the software;

said feedback module writing, to the database, the feedback entries that the feedback module received from the software;

said application firewall preventing the software from accessing the communication network; and

said application firewall ~~permitting the feedback module to~~ controlling access of the communication network~~, said permitting being controlled by the application firewall~~ by the feedback module.

23. (Canceled)

24. (Original) The computer program product of claim 22, wherein the communication network comprises the Internet.

25. (Original) The computer program product of claim 16, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

26. (Currently amended) A process for deploying (or integrating) computing infrastructure, said process comprising integrating computer-readable code into a computing system, wherein the

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 49
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

code in combination with the computing system is capable of performing a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises:

establishing a secret key k(0), ~~that is shared between~~ a feedback module and the vendor sharing the key k(0), and communicating the key k(0) to a user of the software, wherein the user is external to the end user machine;

establishing a secret key n(0), ~~that is shared between~~ the feedback module and the vendor sharing the key n(0), ~~but~~ and not communicating the key n(0) to the user;

a processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database;

said processor, via execution of the feedback module, generating a secret key s(0) and communicating the generated key s(0) to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$;

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that $H_{n0} = Hash(n(0) \| E_{k0})$;

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that $H_{s0} = Hash(s(0) \| E_{k0})$;

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 50
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

27. (Previously presented) The process of claim 26, said method comprising:

said processor, via execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database.

28. (Previously presented) The process of claim 27, said method comprising, said processor, via execution of the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), …, FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, …, N comprising:

calculating parameters E_{ki}, H_{ni}, and H_{si} such that E_{ki} = E(k(i), FE(i)), H_{ni} = Hash(n(i) || E_{ki}), and H_{si} = Hash(s(i) || E_{ki});

writing E_{ki}, H_{ni}, and H_{si} to the database;

generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 51
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

29. (Previously presented) The process of claim 28, said method comprising said processor, via execution of the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

30. (Original) The process of claim29, wherein M=1.

31. (Original) The process of claim 29, wherein M>1.

32. (Currently amended) The process of claim 26, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, <u>wherein the feedback module is connected to both the application firewall and the database, wherein the software is connected to the feedback module, wherein the software is coupled to the application firewall via the feedback module, wherein the software is coupled to the database via the feedback module,</u> and wherein the method further comprises<u>,</u> and wherein the method further comprises<u>:</u>

<u>said feedback module receiving the feedback entries from the software;</u>

<u>said feedback module writing, to the database, the feedback entries that the feedback module received from the software;</u>

<u>said application firewall preventing the software from accessing the communication network; and</u>

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 52
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

said application firewall ~~permitting the feedback module to~~ controlling access of the communication network~~, said permitting being controlled by the application firewall~~ by the feedback module.

33. (Canceled)

34. (Original) The process of claim 32, wherein the communication network comprises the Internet.

35. (Original) The process of claim 26, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 53
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

REMARKS

Applicants have amended claims 1-4, 8-9, 11-12, 16-19, 26-29, and 32, and have cancelled claims 13, 23, and 33, during prosecution of this patent application. Applicants are not conceding in this patent application that the subject matter encompassed by said amended and cancelled claims are not patentable over the art cited by the Examiner, since the claim amendments and cancellations are only for facilitating expeditious prosecution of this patent application. Applicants respectfully reserve the right to pursue the subject matter encompassed by said amended and cancelled claims, and to pursue other claims, in one or more continuations and/or divisional patent applications.

The Examiner rejected claims 1, 12-16, 22-26 and 32-35 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) and further in view of Ginter, et al. (US Patent No. 5,892,900, hereinafter "Ginter") and further in view of Hammersmith (US Patent Application Publication No. 2003/0016821).

The Examiner rejected claims 2-11, 17-21 and 27-31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal in view of Tsudik, in further view of Ginter, in further view of Hammersmith, and further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter "Wheeler").

Applicant respectfully traverses the § 103 rejections with the following arguments.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 54
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 103(a): Claims 1, 12-16, 22-26 and 32-35

The Examiner rejected claims 1, 12-16, 22-26 and 32-35 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) and further in view of Ginter, et al. (US Patent No. 5,892,900, hereinafter "Ginter") and further in view of Hammersmith (US Patent Application Publication No. 2003/0016821).

Since claims 13, 23, and 33 have been cancelled, the rejection of claims 13, 23, and 33 under 35 U.S.C. § 103(a) is moot.

Applicant respectfully contends that claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith, because Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach or suggest each and every feature of claims 1, 16, and 26.

A first example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach or suggest the feature: "establishing a secret key k(0), a feedback module and the vendor sharing the key k(0), and communicating the key k(0) to a user of the software".

The Examiner argues: "Elgamal discloses ... establishing a secret key k(0) that is shared between a feedback module and the vendor (Elgamal **2:1-15; 7:41-51; 8:5-20; 33:9-13)**".

In response, Applicant notes that the Examiner is arguing that the claimed secret key k(0) is represented in Elgamal as a master key that is shared between the client and the server, which is explained in the Examiner's citation of Elgamal, col. 7, lines 41-51. However, Elgamel does

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 55
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

not disclose that the master key has been communicated to a user at the client machine, as required by the preceding feature of claims 1, 16, and 26.

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 1, 16, and 26.

A second example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith is that Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach or suggest the feature: "establishing a secret key n(0), the feedback module and the vendor sharing the key n(0), and not communicating the key n(0) to the user".

The Examiner argues: "Elgamal discloses ... establishing a key that is shared between a feedback module and the vendor, but not communicating the key to the user (Elgamal **23:9-19; 28:38-40; 33:1-4)**".

In response, Applicant respectfully contends that Elgamal does not disclose that the client session key is not communicated to a user of the client machine, as required by the preceding feature of claims 1, 16, and 26.

In "Response to Amendment/Arguments", the Examiner argues: "although Elgamal does not explicitly state that the client session key is not communicated to a user, it also does not state that the key is communicated to a user."

In response, Applicant asserts that a lack of disclosure that the client session key is communicated to a user is not a disclosure that the client session key is not communicated to the user. This is simple logic.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 56
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

MEP § 2173.05(i) explains that, under case law, a negative limitation is not disclosed in a specification unless the negative limitation is positively (or inherently) recited the specification. The logic behind this law also applies to a prior art reference, namely a negative limitation is not disclosed in a prior art reference unless the negative limitation is positively (or inherently) recited in the prior art reference.

Applicant asserts that the negative limitation of "not communicating the key n(0) to the user" is not positively (or inherently) recited in Elgamal. Therefore, Elgamal does not disclose "not communicating the key n(0) to the user".

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 1, 16, and 26.

A third example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "generating an identification tag FE(0) that identifies the software with the vendor".

The Examiner argues: "Elgamal discloses ... generating data ... (Elgamal **3:29-4:67; 27:51-54; 26:41-44; 33:24-32)**".

In response, Applicant asserts that the preceding claimed feature of "generating an identification tag FE(0) that identifies the software with the vendor" is much more limiting than "generating data".

In "Response to Amendment/Arguments", the Examiner argues: "The description of the data in the claim as being an "identification tag" is nonfunctional descriptive material as it only describes stored data, and none of the method steps identify anything using the data."

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 57
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In response, Applicant asserts that claims 1, 16, and 26 recite using the identification tag FE(0) in the step of: "generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$".

Furthermore, the "identification tag FE(0) that identifies the software with the vendor" is not directed towards nonfunctional descriptive material, but rather is being encrypted in relation to a utility of the present invention, namely the utility of protecting the security and privacy of communications from the software to the vendor. See specification, page 6, line 18 - page 7, line 20.

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith and further in view of Hammersmith does not teach the preceding feature of claims 1, 16, and 26.

A fourth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith is that Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach or suggest the feature: "generating a secret key s(0) and communicating the key s(0) to the user but not to the vendor ..., wherein the end user machine comprises the processor, the software, the feedback module, and a database ... software, wherein the user is external to the end user machine".

The Examiner argues:

"Elgamal in view of Tsudik does not specifically disclose ... generating a key known only to the user... Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 58
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

(Ginter **222:50-61).** Ginter further discloses storage of authentication values (Ginter 245:55-62; 246:18-23, 27-50)... Hammersmith discloses using one-time-pad encryption keys for encryption, and providing a user with a display window that allows a user to track the current keys (Hammersmith Paragraph 45).

Therefore, ... it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik to include the user generating a secure database key known only to the PPE and storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter **222:55-57).** Finally, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to include allowing a user to track keys as disclosed in Hammersmith in order to allow the use of one-time-use keys in order to prevent data from being compromised if an encryption key is broken/guessed (Hammersmith Paragraphs 4-6)." (emphasis added).

In response, Applicant notes that the user is outside of a computer (i.e., outside of the end user machine as claimed). The PPE in Ginter is a self-contained computing environment. See Ginter, col. 87, lines 2-11 ("ROS 602 in this example also includes one or more Host Event Processing Environments ("HPEs") 655 and/or one or more Secure Event Processing Environments ("SPEs") 503 (these environments may be generically referred to as "Protected Processing Environments" 650)... HPE(s) 655 and SPE(s) 503 are ***self-contained computing and processing environments*** that may include their own operating system kernel 688 including code and data processing resources.") (emphasis added). Therefore, the user is outside of the PPE.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 59
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Applicant respectfully contends that it is not obvious to communicate to the user (as disclosed by Hammersmith) a key known only to the PPE (as disclosed by Ginter), because Ginter teaches away disclosing the key to any entity outside of the PPE. See Ginter, page 222, lines 50-52 ("PPE 650 preferably generates these secure database keys and ***never exposes them outside of the PPE***.").

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 1, 16, and 26.

A fifth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith is that Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach or suggest the feature: "said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) such that E_{k0}= E(k(0),FE(0))".

The Examiner argues: "Elgamal discloses ... encrypting information to be transferred to the vendor (Elgamal Elgamal 28:41-44, 2:5-10; 7:2-8; 13:17-28; 14:65-68)".

In response, Applicant asserts that the preceding feature of claims 1, 16, and 26 requires that the identification tag FE(0) be encrypted and, although Elgamal discloses encrypting information, Elgamal does not disclose encrypting the identification tag FE(0) that identifies the software with the vendor, as required by the preceding feature of claims 1, 16, and 26.

The Examiner argues: "the description of the data in the claim as being an "identification tag" is nonfunctional descriptive material as it only describes stored data, and none of the method steps identify anything using the data."

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 60
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In response, Applicant notes that the identification tag FE(0) that identifies the software with the vendor is not directed towards nonfunctional descriptive material, but rather is being used by being encrypted as recited: $E_{k0} = E(k(0),FE(0))$. Furthermore as explained *supra*, the "identification tag FE(0) that identifies the software with the vendor" relates to a utility of the present invention, namely the utility of protecting the security and privacy of communications from the software to the vendor. See specification, page 6, line 18 - page 7, line 20.

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 1, 16, and 26.

A sixth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith is that Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach or suggest the feature: "said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that $H_{n0} = \text{Hash}(n(0) \| E_{k0})$; said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that $H_{s0} = \text{Hash}(s(0) \| E_{k0})$".

The Examiner argues:

"Elgamal further discloses the use of a MAC (message authentication code) to verify the integrity of data that is to be transmitted and that the MAC includes a hash of the data and a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27)....** Tsudik discloses the use of the secret prefix method of generating a MAC using a hash function. Tsudik discloses that in this method, two principals agree on a secret, S_ab for example, and when A sends a message M to B, it generates an MD4 hash of S_ab concatenated

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 61
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

to the beginning of the message such that HashValue = MD4Hash(S_ab || M). The receiver would then use its knowledge of S_ab and the received message to recompute the hash value and compare it to the received hash value to verify the integrity of the message (Tsudik p. 32, Protocol Description; pp. **33-34** Secret Prefix)."

In response, Applicant asserts that, if the keys n(0) and s(0) are used as the "secret" in Elgamal and the "secret prefix" in Tsudick, then the preceding feature of claims 1, 16, and 26 requires that E_{k0} be the "data" or "message" to be transmitted. However, Elgamal does not disclose transmitting E_{k0}. In fact, there is no disclosure in Elgamal, Tsudik, or Ginter of the existence of E_{k0}, namely an encryption of the identification tag (that identifies the software with the vendor) using the key k(0).

In further response, Applicant acknowledges that the Examiner has shown via Tsudick that it is known to compute of a hash of an argument consisting of a secret concatenated with a message. However, the Examiner has not cited any prior art allegedly disclosing computing the two specific hashes of E_{k0} being claimed, namely Hash(n(0) || E_{k0}) and Hash(s(0) || E_{k0}).

Furthermore, the Examiner has not provided a reason as to why it is allegedly obvious to modify Elgamal to compute the two specific hashes of E_{k0} being claimed, namely Hash(n(0) || E_{k0}) and Hash(s(0) || E_{k0}).

Thus, the Examiner has not established a *prima facie* case of obviousness in relation to claims 1, 16, and 26.

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 62
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

A seventh example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith is that Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach or suggest the feature: "said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor".

The Examiner argues: "Ginter further discloses storage of authentication values (Ginter **245:55-62; 246:18-23, 27-50)...** Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik to include ... storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter 222:55-57)."

In response and assuming that storing E_{k0}, H_{n0}, and H_{s0} in the user's database would protect data in the user's database from be accessed by another party (for the sake of argument only), Applicant asserts that the Examiner's reason for modifying Elgamal in view of Tsudik to store E_ko and Hno in the user's database ("to be able to securely store data that cannot be accessed by another party in a database at the user's device") is negated by the claimed limitation. "sending E_{k0} and H_{n0} to the vendor" which would enable the vendor to access the very authentication data in the user's device that is intended to be protected from such access.

Thus, the Examiner's argument is not persuasive.

Furthermore, the Examiner has not addressed the limitation of "said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor". Thus, the Examiner has not established a *prima facie* case of obviousness in relation to claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 63
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 1, 16, and 26.

Based on the preceding arguments, Applicant respectfully maintains that claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter, and further in view of Hammersmith and that claims 1, 16, and 26 are in condition for allowance. Since claims 12 and 14-15 depend from claim 1, Applicant contends that claims 12 and 14-15 are likewise in condition for allowance. Since claims 22 and 24-25 depend from claim 16, Applicant contends that claims 22 and 24-25 are likewise in condition for allowance. Since claims 32 and 34-35 depend from claim 26, Applicant contends that claims 32 and 34-35 are likewise in condition for allowance.

In addition with respect to claims 12, 22, and 32, Elgamal in view of Tsudik and further in view of Ginter, and further in view of Hammersmith does not disclose the feature:

"wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, wherein the feedback module is connected to both the application firewall and the database, wherein the software is connected to the feedback module, wherein the software is coupled to the application firewall via the feedback module, wherein the software is coupled to the database via the feedback module, and wherein the method further comprises:

said feedback module receiving the feedback entries from the software;

said feedback module writing, to the database, the feedback entries that the feedback module received from the software;

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 64
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

said application firewall preventing the software from accessing the communication network; and

said application firewall controlling access of the communication network by the feedback module".

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 12, 22, and 32.

In addition with respect to claims 15, 25, and 35, Elgamal in view of Tsudik and further in view of Ginter, and further in view of Hammersmith does not disclose the feature: "wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software".

The Examiner admits: "Elgamal in view of Tsudik in further view of Ginter does not specifically disclose that the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software."

The Examiner argues: "However, as the description of the identification tag does not affect the method steps, this is directed towards nonfunctional descriptive material and thus does not serve to differentiate the claims from the prior art. It has been held that where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability .... [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 65
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

substrate *(In re Gulack,* 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai,* 70 USPQ2d (Fed. Cir. 2004), *In re Lowry, 32* USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II)."

In response, Applicant notes that the identification tag FE(0) that identifies the software with the vendor is not directed towards nonfunctional descriptive material, but rather is being used by being encrypted as recited: $E_{k0} = E(k(0),FE(0))$. Furthermore as explained *supra*, the "identification tag FE(0) that identifies the software with the vendor" relates to a utility of the present invention, namely the utility of protecting the security and privacy of communications from the software to the vendor. See specification, page 6, line 18 - page 7, line 20.

Therefore, Elgamal in view of Tsudik and further in view of Ginter and further in view of Hammersmith does not teach the preceding feature of claims 12, 22, and 32.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 66
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 103(a): Claims 2-11, 17-21 and 27-31

The Examiner rejected claims 2-11, 17-21 and 27-31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal in view of Tsudik, in further view of Ginter, in further view of Hammersmith, and further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter "Wheeler").

Since claims 2-11 depend from claim 1, which Applicant has argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further view of Hammersmith under 35 U.S.C. § 103(a), Applicant maintains that claims 2-11 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

Since claims 17-21 depend from claim 1, which Applicant has argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further view of Hammersmith under 35 U.S.C. § 103(a), Applicant maintains that claims 17-21 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

Since claims 27-31 depend from claim 1, which Applicant has argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter and further view of Hammersmith under 35 U.S.C. § 103(a), Applicant maintains that claims 27-31 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 67
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In addition with respect to claims 2, 17, and 27, Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith, and further in view of Wheeler does not disclose the feature: "said processor, via

execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database"

The Examiner argues: "Regarding claims 2, 3, 17, 18, 27 and 28, ... Elgamal in view of Tsudik in further view of Ginter does not specifically disclose generating a series of keys in which a new key is generated by hashing the last key and using the keys to generate a series of hash values... Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68)...** Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to include computing a series of keys used to encrypt blocks of data as disclosed in Wheeler in order to allow the data to be transferred using broadcast transmission (Wheeler Paragraph 53)".

In response, Applicant asserts that Wheeler does not anywhere disclose that the generation of keys as claimed (i.e., that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0))) is needed to encrypt blocks of data in order to allow the data to be transferred using broadcast transmission. Applicant asserts that the ability to encrypt blocks of data in order to allow the data to be transferred using broadcast transmission does not depend on any particular method of generating the keys used for the encryptions.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 68
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Accordingly, Applicant respectfully contends that it is not obvious to modify Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith by generation of keys as claimed (i.e., that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0))) for encrypting blocks of data in order to allow the data to be transferred using broadcast transmission.

Therefore, claims 2, 17, and 27 are not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

In addition with respect to claims 3, 18, and 28, Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith, and further in view of Wheeler does not disclose the feature: "for each of i = 1, …, N ... : ... said processor, via execution of the feedback module, generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i))".

The Examiner argues: "Regarding claims 2, 3, 17, 18, 27 and 28, ... Elgamal in view of Tsudik in further view of Ginter does not specifically disclose generating a series of keys in which a new key is generated by hashing the last key and using the keys to generate a series of hash values... Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68)...** Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to include computing a series of

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 69
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

keys used to encrypt blocks of data as disclosed in Wheeler in order to allow the data to be transferred using broadcast transmission (Wheeler Paragraph 53)".

In response, Applicant asserts that Wheeler does not anywhere disclose that generating a series of keys (in which a new key is generated by hashing the last key and using the keys to generate a series of hash values) is needed to encrypt blocks of data in order to allow the data to be transferred using broadcast transmission. Applicant asserts that the ability to encrypt blocks of data in order to allow the data to be transferred using broadcast transmission does not depend on any particular method of generating the series of keys used for the encryptions.

Accordingly, Applicant respectfully contends that it is not obvious to modify Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith by generating a series of keys (in which a new key is generated by hashing the last key and using the keys to generate a series of hash values) for encrypting blocks of data in order to allow the data to be transferred using broadcast transmission.

In addition, Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler does not disclose the feature:

"for each of i = 1, …, N … :

calculating parameters E_{ki}, H_{ni}, and H_{si} such that $E_{ki} = E(k(i), FE(i))$, $H_{ni} = Hash(n(i) \| E_{ki})$, and $H_{si} = Hash(s(i) \| E_{ki})$;

writing E_{ki}, H_{ni}, and H_{si} to the database; …

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1)".

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 70
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, claims 3, 18, and 28 are not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

In addition with respect to claims 4, 19, and 29, Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith, and further in view of Wheeler does not disclose the feature: "synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$".

The Examiner argues: "Regarding claims 4-6, 19-21, and 29-31, Elgamal discloses generating a key by the user terminal that is used for encryption by the vendor (Elgamal **23:9-19; 28:38-40; 33:1-4)** and encrypting information and transferring it to the vendor (Elgamal **2:5-10; 7:2-8; 8:9-11; 7:62-8:4; 13:17-28; 14:65-68).** Wheeler further discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68).**"

In response, Applicant respectfully contends that Elgamal, col. 2, lines 5-10; col. 7, lines 2-8; col. 8, lines 9-11; col. 7 line 62 - col. 8, line 4; col. 13, lines 17-28; and coil. 14, lines 65-68 do not disclose sending to the vendor specifically (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 71
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, claims 4, 19, and 29 are not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

In addition with respect to claims 7 and 10, Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith, and further in view of Wheeler does not disclose the feature: "verifying, by the vendor, an integrity of the N feedback entries received by the vendor as a result of said sending to the vendor: $((E_{ki}, H_{ni}), i = M, \ldots, N)$ and $E(k(N+1), n(N+1))$, wherein $1 \leq M \leq N$".

The Examiner argues: "Regarding claims 7 and 10 Elgamal discloses the use of a MAC (message authentication code) to verify the integrity of data and that the MAC includes a hash of the data as well as a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27).** Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database (Ginter **222:50-61).** Ginter further discloses storage of authentication values (Ginter **245:55-62; 246:18-23, 27-50).**"

In response, Applicant respectfully contends that the preceding argument by the Examiner does not persuasively explain how Elgamel and Ginter allegedly discloses "verifying, by the vendor, an integrity of the N feedback entries received by the vendor as a result of said sending to the vendor: $((E_{ki}, H_{ni}), i = M, \ldots, N)$ and $E(k(N+1), n(N+1))$, wherein $1 \leq M \leq N$".

Therefore, claims 7 and 10 are not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 72
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In addition with respect to claim 8, Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith, and further in view of Wheeler does not disclose the feature: "wherein said verifying comprises:

setting $i = 0$ and $H(0) = n(0)$;

executing iterations $i = 0, 1, \ldots, N$ of a loop, wherein executing each iteration i of the loop comprises: setting $H'_{ni} = \mathrm{Hash}(H(i) \| E_{ki})$; determining that $H'_{ni} = H_{ni}$; and responsive to said determining that $H'_{ni} = H_{ni}$, setting $H(i+1) = \mathrm{Hash}(H(i))$ and $k(i+1) = \mathrm{Hash}(k(i))$;

after said executing:

decrypting $E(k(N+1), n(N+1))$ using key $k(N+1)$ to infer $n(N+1)$;

determining that $n(N+1) = H(N+1)$; and

responsive to said determining that $n(N+1) = H(N+1)$, ascertaining that the integrity of the N feedback entries received by the vendor has been verified".

The Examiner argues: "Regarding claims 8-9 and 11, Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68).** Wheeler discloses verifying whether a received key is valid by comparing the received key to a key independently generated by the recipient by hashing the previously received key (Wheeler Paragraph **57).**"

In response, Applicant respectfully contends that the preceding argument by the Examiner does not persuasively explain how Wheeler allegedly discloses the preceding feature of claim 8.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 73
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, claim 8 is not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

In addition with respect to claim 9, Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith, and further in view of Wheeler does not disclose the feature: "wherein the validation method further comprises, as performed by the vendor prior to said verifying:

calculating $H'_{n0} = \text{Hash}(n(0) \| E_{k0})$;

determining that $H'_{n0} = H_{n0}$; and

responsive to said determining that $H'_{n0} = H_{n0}$, decrypting E_{ko} to infer FE(0) and recording that the database is set".

The Examiner argues: "Regarding claims 8-9 and 11, Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68).** Wheeler discloses verifying whether a received key is valid by comparing the received key to a key independently generated by the recipient by hashing the previously received key (Wheeler Paragraph **57).**"

In response, Applicant respectfully contends that the preceding argument by the Examiner does not persuasively explain how Wheeler allegedly discloses the preceding feature of claim 9.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 74
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, claim 9 is not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

In addition with respect to claim 11, Elgamal in view of Tsudik, in further view of Ginter and further in view of Hammersmith, and further in view of Wheeler does not disclose the feature: "wherein said verifying comprises:

setting $i = 0$ and $S(0) = s(0)$;

executing iterations $i = 0, 1, \ldots, N$ of a loop, wherein executing each iteration i of the loop comprises: setting $H'_{si} = \text{Hash}(S(i) \| E_{ki})$; determining that $H'_{si} = H_{si}$; and responsive to said determining that $H'_{si} = H_{si}$, setting $S(i+1) = \text{Hash}(S(i))$;

after said executing:

determining that $S(N+1) = s(N+1)$; and

responsive to said determining that $S(N+1) = s(N+1)$, ascertaining that the integrity of the N feedback entries in the database has been verified".

The Examiner argues: "Regarding claims 8-9 and 11, Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68).** Wheeler discloses verifying whether a received key is valid by comparing the received key to a key independently generated by the recipient by hashing the previously received key (Wheeler Paragraph **57).**"

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 75
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In response, Applicant respectfully contends that the preceding argument by the Examiner does not persuasively explain how Wheeler allegedly discloses the preceding feature of claim 11.

Therefore, claim 11 is not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further view of Hammersmith, and further in view of Wheeler under 35 U.S.C. §103(a).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 76
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

CONCLUSION

Based on the preceding arguments, Applicant respectfully believes that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicant invites the Examiner to contact Applicant's representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account 09-0457 (IBM).

Date: January 28, 2010

/ Jack P. Friedman /
Jack P. Friedman
Registration No. 44,688

Customer No. 30449
Schmeiser, Olsen & Watts
22 Century Hill Drive - Suite 302
Latham, New York 12110
Telephone (518) 220-1850
Facsimile (518) 220-1857
Email: jfriedman@iplawusa.com

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 77
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. 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	Filing Date	☐ To be Mailed
11/325,719	01/05/2006	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		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))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 01/28/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 32	Minus	** 35	= 0	X $ =		OR	X $52=	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $ =		OR	X $220=	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

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							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:
/ERIC V. BURNS/

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.
11/325,719	01/05/2006	Vijil Enara Chenthamarakshan	IN920050028US1	7235

30449 7590 11/03/2009
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER
NILFOROUSH, MOHAMMAD A

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
11/03/2009	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.	Applicant(s)	
	11/325,719	CHENTHAMARAKSHAN, VIJIL ENARA	
	Examiner	**Art Unit**	
	Mohammad A. Nilforoush	3685	

-- 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 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* 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 _____ 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)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 80
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

DETAILED ACTION

Acknowledgements

1. The amendment filed 1 July 2009 is acknowledged.

2. Claims 1-35 are pending.

3. Claims 1-35 have been examined.

4. This Office action is given Paper No. 20091025 for reference purposes only.

Response to Amendment/Arguments

5. The amendment of claims 1, 16 and 26 overcomes the rejection of claims 1-35 under 35 USC §101.

6. The amendment of claims 1, 16, and 26 overcomes the rejection of claims of 1-35 under 35 USC §112, second paragraph.

7. The claims have been amended to recite language that does not serve to differentiate the claims from the prior art. Claims 1, 16, and 26 recite "...a secret key k(0) *that is shared...*" and "...a secret key n(0) *that is shared*..." However, as there is no positively recited step of "sharing" the keys, this language does not require that the keys be shared between a feedback module and a vendor. The recitation of the intended use of the claimed invention does not serve to differentiate the invention from the prior art. MPEP §2106 II C states that language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. An example of such language includes statements of intended use or field of use (MPEP §2106 II C).

8. It is the Applicant's position that "*…the client session key and the server session key are distinct keys that are separately generated by the client and the server, respectively, and are thus not shared between the client and the server…*" and "*…Elgamal does not disclose that the client session key is not communicated to a user of the client machine…*"

9. Examiner respectfully disagrees. Although the client and server session key are generated separately, Elgamal discloses that they are the same key, i.e. the client write key is the same as the server read key (both key 1), or the client read key is the same as the server write key (both key 2) (Elgamal **28:36-40**). Also, the data that the keys are composed of is transmitted from the client to the server (Elgamal **27:64-28:45**). Additionally, although Elgamal does not explicitly state that the client session key is not communicated to a user, it also does not state that the key is communicated to a user. Further, Elgamal describes that the communication between the client and server, along with the encryption and decryption of the data transferred between them, occurs using the SSL library, which emulates the sockets API (application programming interface) (Elgamal **5:18-39**). Elgamal also discloses that the sockets API serves as an interface used by applications to communicate with the TCP/IP protocol stack, and that the sockets API provides system calls invoked by application programs (Elgamal **5:40-54**). Also, the SSL library is layered between the application layer programs and the operating system transport control protocol stack (Elgamal **6:30-34**). Thus, the operation of the SSL library and sockets API does not involve any output to the user via a graphical user interface.

10. Applicant also states that: "*…Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: 'generating an identification tag FE(0) that identifies the software with the vendor'.*"

11. Examiner respectfully disagrees. Elgamal discloses producing various types of data (Elgamal **3:29-45**; **28:41-44**; **33:24-32**) as well as encrypting it. Data is encrypted both using the master key (Elgamal **28:41-44**) and using the session keys (Elgamal **2:5-10**; **7:2-8**; **8:9-11**; **7:62-8:4**; **13:17-28**; **14:65-68**). The description of the data in the claim as being an "identification tag" is nonfunctional descriptive material as it only describes stored data, and none of the method steps identify anything using the data. Nonfunctional descriptive material does not serve to differentiate the claims from the prior art. It has been held that where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability …. [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate (*In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II). Further, the limitation that the identification tag "...identifies the software with the vendor" is a statement of the intended use of the data. Recitations of intended use do not serve to differentiate the claims from the prior art. MPEP §2106 II C states that language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. An example of such language includes statements of intended use or field of use (MPEP §2106 II C).

12. Also, Applicant states that "*…Ginter does not explain the meaning of 'PPE' and Applicants do not know what a PPE is in Ginter…*"

13. Ginter describes a PPE as being a "Protected Processing Environment". PPE's can be either Host Event Processing Environments or Secure Even Processing Environments. They are self-contained computing and processing environments that may include their own operating system kernel. PPE's are supported by the processor of the electronic device in which they are located. The PPE's, HPE's, and SPE's of Ginter are further described in col. 86, line 63 to col. 88, line 11 and col. 112, lines 1-67.

14. Additionally, Applicant states: "*[a] second reason why the Examiner's suggested modification Elgamal is not persuasive is that the Examiner's argument asserts that modifying Elgamal…enables the use of encryption to be avoided. However, the use of encryption is within the essence of Elgamal's invention (see Elgamal, abstract and claim 1).*"

15. Examiner respectfully disagrees. The Office action states on page 8 that the motivation for modifying Elgamal with Tsudik was in order to produce integrity values (i.e. message authentication codes) without using encryption, not to eliminate encryption altogether from Elgamal.

16. Applicant also contends that "*…the Examiner's argument is specific to the use of databases. However, Elgamal's invention does not relate to the use of a database.*"

17. However, the invention of Elgamal can be applied to any type of application program that involves transferring data between a client and a server (Elgamal **1:58-2:2**; **3:24-45**; **11:58-12:13**). Further, a database is defined as a collection of data

arranged for ease and speed of search and retrieval (The American Heritage Dictionary of the English Language, 4th Ed., 2000) and Elgamal discloses retrieving data from servers via links on an HTML page (Elgamal **3:56-4:67**). Thus, the invention of Elgamal relates to the use of databases.

18. Applicant also states that *"…Elgamal does not disclose encrypting the identification tag FE(0) that identifies the software with the vendor…"* Additionally, Applicant is of the position that "*...Elgamal does not disclose transmitting Ek0. In fact, there is no disclosure in Elgamal, Tsudik, or Ginter of the existence of Ek0, namely an encryption of the identification tag (that that identifies the software with the vendor) using the key k(0).*"

19. However, as described previously, Elgamal discloses producing various types of data (Elgamal **3:29-45**; **27:51-54**; **28:41-44**; **33:24-32**) as well as encrypting it. Data is encrypted both using the master key (Elgamal **28:41-44**) and using the session keys (Elgamal **2:5-10**; **7:2-8**; **8:9-11**; **7:62-8:4**; **13:17-28**; **14:65-68**). Further, as described above, the description of the data in the claim as being an "identification tag" is nonfunctional descriptive material and the limitation that the identification tag "...identifies the software with the vendor" is a statement of the intended use of the data. Nonfunctional descriptive material and intended use language do not serve to differentiate the claims from the prior art.

20. Applicant further contends that *"…Elgamal does not disclose that the encryption of information in Elgamal is performed through use of the master key.*"

21. However, Elgamal discloses encrypting information using the master key (Elgamal **28:41-44**).

22. Applicant also states that "*However…the key s(0) is not communicated to the vendor (i.e., the server in Elgamal). Therefore, it is logically impossible to satisfy the requirement of the key s(0) not being communicated to the vendor if Tsudik's 'secret prefix' method is used to modify Elgamal.*"

23. Tsudik discloses that the random value must be communicated between the two principals who want to communicate a message and verify the integrity of the message the authentication using the generated hash. Thus, as Hs0 is not communicated to the vendor/server, there is not need for the server to know the key s(0). Rather, only the entity that will receive the message (Ek0) and hash (Hs0) (i.e., the user of the database) needs to be sent the key s(0) so as to be able to generate a hash of s(0) and the received Ek0 independently and compare it to the received, original Hs0 to verify that the received Ek0 has not been modified.

24. Further, it is the Applicant's position that "*…it is not clear that storing Eko, Hn0,and Hs0 in the user's database would protect data in the user's database from be accessed by another party…*" and "*…the Examiner's reason for modifying Elgamal in view of Tsudik to store Ek0 and Hn0 in the user's database…is negated by the claimed limitation 'sending Ek0 and Hn0 to the vendor' which would enable the vendor to access the very data in the user's device that is intended to be protected from such access by storing Ek0 and Hn0 in the user's database in the first place.*"

25. Examiner respectfully disagrees. Ginter discloses that data stored in a secure database is encrypted and the encryption keys are kept in a secure location (Ginter **222:50-61**; **245:55-62**; **246:18-23**, **27-50**). Thus, unauthorized users of a PPE are prevented from accessing the database. Further, although copies of Ek0 and Hn0 are sent to the vendor in the claim, the vendor does not access these variables from the database, but receives a separate copy from the feedback module. Further, the claim does not require that the vendor access data, such as Hs0, that is stored solely in the database.

26. Additionally, Applicant states that "*…the Examiner cites Wheeler for modifying Elgamal 'to encrypt blocks of data'. Yet, the Examiner cites Tsudik 'to use the secret prefix method ... without using encryption'. Thus, the Examiner's reliance on Wheeler is inconsistent with the Examiner's reliance on Tsudik.*"

27. Examiner respectfully disagrees. As described previously, the modification of Elgamal with Tsudik was in order to produce integrity values (i.e. message authentication codes) used to verify the integrity of transmitted data without using encryption, not to eliminate encryption of the actual data that is transmitted.

28. Applicant's remaining arguments with respect to claims 1-35 have been considered but are moot in view of the new ground(s) of rejection.

29. Additionally, regarding claims 12-13, 21-23, and 32-33, the use of a firewall to permit or prevent a machine to access a network is considered to be admitted prior art as Applicant did not traverse Examiner's assertion that such a feature is old and well-known.

Claim Rejections - 35 USC § 103

30. 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 negatived by the manner in which the invention was made.

31. Claims 1, 12-16, 22-26, and 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) in further view of Ginter, et al. (US Patent No. 5,892,900, hereinafter "Ginter") and further in view of Hammersmith (US Patent Application Publication No. 2003/0016821)

32. Regarding claims 1, 16, and 26 Elgamal discloses

establishing a secret key k(0) that is shared between a feedback module and the vendor (Elgamal **2:1-15**; **7:41-51**; **8:5-20**; **33:9-13**);

establishing a key that is shared between a feedback module and the vendor, but not communicating the key to the user (Elgamal **23:9-19**; **28:38-40**; **33:1-4**);

generating data, wherein the end user machine comprises the processor, the software, the feedback module, and a database (Elgamal **3:29-4:67**; **27:51-54**; **28:41-44**; **33:24-32**);

encrypting information to be transferred to the vendor using the key k(0) (Elgamal Elgamal **28:41-44**; **2:5-10**; **7:2-8**; **13:17-28**; **14:65-68**)

Elgamal further discloses the use of a MAC (message authentication code) to verify the integrity of data that is to be transmitted and that the MAC includes a hash of the data and a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27**).

Elgamal does not specifically disclose communicating a key k(0) to a user of the software or generating a key known only to the user. Elgamal also does not explicitly state that hash values used to verify the integrity of the data comprise a hash of the data to be transmitted concatenated with the key of the client or server respectively, that the encrypted data is stored at the client, or that the generated data is an identification tag that identifies the software with the vendor.

Tsudik discloses the use of the secret prefix method of generating a MAC using a hash function. Tsudik discloses that in this method, two principals agree on a secret, S_ab for example, and when A sends a message M to B, it generates an MD4 hash of S_ab concatenated to the beginning of the message such that HashValue = MD4Hash(S_ab || M). The receiver would then use its knowledge of S_ab and the received message to recompute the hash value and compare it to the received hash

value to verify the integrity of the message (Tsudik p. **32**, Protocol Description; pp. **33-34** Secret Prefix).

Elgamal in view of Tsudik does not specifically disclose communicating a key k(0) to a user of the software, generating a key known only to the user or that the encrypted data is stored at the client. Elgamal in view of Tsudik further does not specifically disclose that the generated data is an identification tag that identifies the software with the vendor.

Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database (Ginter **222:50-61**). Ginter further discloses storage of authentication values (Ginter **245:55-62**; **246:18-23**, **27-50**).

Elgamal in view of Tsudik in further view of Ginter does not specifically disclose communicating a key k(0) to a user of the software.

Hammersmith discloses using one-time-pad encryption keys for encryption, and providing a user with a display window that allows a user to track the current keys (Hammersmith Paragraph 45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal to use the secret prefix method of generating a message authentication code in order to produce unforgeable integrity values without using encryption so as to provide increased speed by minimizing the use of encryption software (Tsudik pp. **30-31** Motivation). Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the

method of Elgamal in view of Tsudik to include the user generating a secure database key known only to the PPE and storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter **222:55-57**). Finally, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to include allowing a user to track keys as disclosed in Hammersmith in order to allow the use of one-time-use keys in order to prevent data from being compromised if an encryption key is broken/guessed (Hammersmith Paragraphs **4-6**). Additionally, the description of the data in the claim as being an "identification tag" is nonfunctional descriptive material as it only describes stored data, and none of the method steps identify anything using the data. Nonfunctional descriptive material does not serve to differentiate the claims from the prior art. It has been held that where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability …. [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate (*In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II). Further, the limitation that the identification tag "...identifies the software with the vendor" is a statement of the intended use of the data. Recitations of intended use do not serve to differentiate the claims from the prior art. MPEP §2106 II C states that language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a

particular structure does not limit the scope of a claim or claim limitation. An example of such language includes statements of intended use or field of use (MPEP §2106 II C).

33. Regarding claims 12-13, 21-23, and 32-33, Elgamal discloses that a communication network is disposed between the end user machine and the vendor, and permitting the user's machine to access the communication network (Elgamal Abstract **3:24-45**; **4:6-12**; **5:44-50**),

Elgamal does not specifically disclose that an application firewall is disposed between the end user machine and the communication network, that said permitting is controlled by the application firewall, or preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

However, the use of a firewall to permit or prevent a machine to access a network is old and well-known. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter, in further view of Hammersmith to employ a firewall to control access of client machines to a network in order to prevent unauthorized or excessive use of the network.

34. Regarding claims 14, 24, and 34, Elgamal discloses the method of claim 12, wherein the communication network comprises the Internet (Elgamal **3:24-45**; **4:6-12**; **5:44-50**).

35. Regarding claims 15, 25, and 35, Elgamal in view of Tsudik in further view of Ginter does not specifically disclose that the identification tag is selected from the group

consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

However, as the description of the identification tag does not affect the method steps, this is directed towards nonfunctional descriptive material and thus does not serve to differentiate the claims from the prior art. It has been held that where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability …. [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate (*In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II).

36. Claims 2-11, 17-21, and 27-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Tsudik, in further view of Ginter, in further view of Hammersmith, and further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter “Wheeler”).

37. Regarding claims 2, 3, 17, 18, 27 and 28, Elgamal discloses storing keys in a database at the user terminal (Elgamal **8:33-53**; **16:23-28**), Tsudik discloses the use of the secret prefix method of generating a MAC using a hash function such that HashValue = MD4Hash(S_ab || M) (Tsudik p. **32**, Protocol Description; pp. **33-34** Secret

Prefix), and Ginter discloses discloses storage of authentication values (Ginter **245:55-62**; **246:18-23**, **27-50**).

Elgamal in view of Tsudik in further view of Ginter, in further view of Hammersmith does not specifically disclose generating a series of keys in which a new key is generated by hashing the last key and using the keys to generate a series of hash values.

Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50**, **55-59**, **66-68**).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter, in further view of Hammersmith to include computing a series of keys used to encrypt blocks of data as disclosed in Wheeler in order to allow the data to be transferred using broadcast transmission (Wheeler Paragraph **53**).

38. Regarding claims 4-6, 19-21, and 29-31,Elgamal discloses generating a key by the user terminal that is used for encryption by the vendor (Elgamal **23:9-19**; **28:38-40**; **33:1-4**) and encrypting information and transferring it to the vendor (Elgamal **2:5-10**; **7:2-8**; **8:9-11**; **7:62-8:4**; **13:17-28**; **14:65-68**). Wheeler further discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each

key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50**, **55-59**, **66-68**).

39. Regarding claims 7 and 10 Elgamal discloses the use of a MAC (message authentication code) to verify the integrity of data and that the MAC includes a hash of the data as well as a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27**). Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database (Ginter **222:50-61**). Ginter further discloses storage of authentication values (Ginter **245:55-62**; **246:18-23**, **27-50**).

40. Regarding claims 8-9 and 11, Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50**, **55-59**, **66-68**). Wheeler discloses verifying whether a received key is valid by comparing the received key to a key independently generated by the recipient by hashing the previously received key (Wheeler Paragraph **57**).

Conclusion

41. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). 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 date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad A. Nilforoush whose telephone number is (571)270-5298. The examiner can normally be reached on Monday-Thursday 8 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on (571)272-6709. 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.

/M. A. N./
Examiner, Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 11/325,719	Applicant(s)/Patent Under Reexamination CHENTHAMARAKSHAN, VIJIL	
	Examiner Mohammad A. Nilforoush	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0016821 A1	01-2003	Hammersmith, Wolfgang	380/37
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Definition of "Database", The American Heritage Dictionary of the English Language, 4th Ed., 2000
	V	
	W	
	X	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	MOHAMMAD NILFOROUSH	3685

✓	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	03/17/2009								
	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	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	MOHAMMAD NILFOROUSH	3685

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	Mohammad A Nilforoush	3685

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
Keyword search (see EAST search history)	3/27/2009	/M. A. N./
Search of relevant references (see EAST search history)	3/27/2009	/M. A. N./
Citation search of relevant references (see EAST search history)	3/27/2009	/M. A. N./
Inventor name search (see EAST search history)	3/27/2009	/M. A. N./
Updated Search (see EAST search history)	10/28/2009	/M. A. N./

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/M. A. N./ Examiner.Art Unit 3685	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S87	1	(US-5892900-$).did.	USPAT	OR	ON	2009/10/26 19:30
S91	1	S87 and (user with (key))	USPAT	OR	ON	2009/10/26 19:31
S90	0	S87 and (user with (database adj key))	USPAT	OR	ON	2009/10/26 19:31
S89	0	S87 and (user with (database near key))	USPAT	OR	ON	2009/10/26 19:31
S88	0	S87 and (user with (access $3 display$3) with (database near key))	USPAT	OR	ON	2009/10/26 19:31
S92	1	("20070299742").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/10/26 19:48
S95	1	S93 and ((present$3 display$3 provid$3 known knowledge output$4) near key with (user administrator client person owner distributor provider enduser))	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:39
S94	1	S93 and ((present$3 display$3 provid$3 known knowledge output$4) near key with (user administrator client person owner distributor provider))	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:39
S93	1	("5892900").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/10/28 19:39
S97	5424	(display$3 present$3 output$4) near key with (user consumer customer)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:49
S96	52767	(display$3 present$3 output$4) with key with (user consumer customer)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:49
S98	13	S97 same (((user client consumer customer) near (terminal computer workstation)) with (generat$3 produc$3) with key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:50

S99	1132	((display$3 present$3 output$4) near key) near2 (user consumer customer)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:56
S102	3	S99 and (((user client consumer customer) near (terminal computer workstation)) with (generat$3 produc$3) near key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:57
S101	0	S99 same (((user client consumer customer) near (terminal computer workstation)) with (generat$3 produc$3) near key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:57
S100	6	S97 same (((user client consumer customer) near (terminal computer workstation)) with (generat$3 produc$3) near key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:57
S104	6	display$3 adj (encryption adj key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:59
S103	6759	display$3 adj (key (encryption adj key))	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 19:59
S110	91	(loyalty adj (card account)) and (target$4 adj (ad advertisement))	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 20:21
S116	392	(send$3 print$3 display $3) adj (encryption adj key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:02
S117	6	display$3 adj (encryption adj key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:03
L4	21	((print$3 display$3) adj (encryption adj key))	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:05
L3	386	L1 not L2	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:05
L2	6	display$3 adj (encryption adj key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:05
L1	392	(send$3 print$3 display $3) adj (encryption adj key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:05

L6	71	(display$3 adj (key)) same (key with (encrypt $3 decrypt$3 cryptograph $6))	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:11
L5	6754	display$3 adj (key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:11
L8	70	l6 not (l2 l4)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:12
L7	70	l6 not (l2, l4)	US-PGPUB; USPAT; USOCR	OR	ON	2009/10/28 22:12

10/28/2009 10:39:00 PM
C:\ Documents and Settings\ mnilforoush\ My Documents\ EAST\ Workspaces\ Mohammad \ 11325719.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Vijil Enara Chenthamarakshan

Group Art Unit: 3685 / Conf. # 7235

Application No.: 11/325,719

Examiner: Nilforoush, Mohammed A.

Filing Date: 01/05/2006

Docket No.: IN920050028US1

Title: SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

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

OFFICE ACTION RESPONSE

Sir:

This communication is in response to the Office Action mailed April 1, 2009.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 105
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In the Specification:

Replacement sheet for Sheet 5 of the drawings is included herewith.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 106
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In the Specification:

The paragraph beginning on page 12, line 17 is amended as follows:

FIG. 5 is a flow charting depicting steps 41 and 42 of FIG. 4, wherein steps 41-42 generate the secret keys k(0) and n(0) (step 41) and s(0) (step 42). The flow chart of FIG. 5 comprises steps 51-55. Step 51 generates the secret keys k(0) and n(0). Step 52 sends the generated secret keys k(0) and n(0) to the vendor 18 securely and communicates the secret key k(0) to the user 19 but does not communicate the secret key n(0) to the user 19. Step 53 prompts the user 19 for a password "P". Step 54 generates the secret key s(0) as a hash of the password P (i.e., as Hash(P)). Step 55 ~~sends k(0) and n(0)~~ communicates the secret key s(0) to the ~~vendor 18 securely~~ user 19, but does not communicate the secret key s(0) to the vendor 18. ~~Although FIG. 5 depicts step 55 after steps 53 and 54, step 55 may be performed either before or after steps 53 and 54.~~

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 107
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In the Claims:

Please cancel claims 14, 24, and 34. Please amend claims 1-4, 8-9, 11, 16-19, and 26-29. The claims are as follows:

1. (Currently amended) A method for processing feedback entries received from software, said software provided by a vendor to an end user machine~~, said end user machine comprising the software, a feedback module, and a database~~, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises ~~comprising, as performed by the feedback module~~:

establishing ~~generating~~ a secret key k(0) ~~and~~ that is shared between a feedback module and the vendor and communicating ~~making~~ the key k(0) ~~known~~ to ~~both the vendor and~~ a user of the software;

establishing ~~generating~~ a secret key n(0) ~~and~~ that is shared between the feedback module and the vendor but not communicating ~~making~~ the key n(0) ~~known to the vendor but not~~ to the user;

a processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database;

said processor, via execution of the feedback module, generating a secret key s(0) and ~~making~~ communicating the key s(0) ~~known~~ to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 108
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

[[an]] the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$;

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that $H_{n0} = Hash(n(0) \| E_{k0})$;

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that $H_{s0} = Hash(s(0) \| E_{k0})$;

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

2. (Currently amended) The method of claim 1, said method comprising~~, as performed by the feedback module~~:

said processor, via execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database.

3. (Currently amended) The method of claim 2, said method comprising~~, as performed by the feedback module,~~ said processor, via execution of the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), …, FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, …, N comprising:

calculating parameters E_{ki}, H_{ni}, and H_{si} such that $E_{ki} = E(k(i), FE(i))$, $H_{ni} = Hash(n(i) \| E_{ki})$, and $H_{si} = Hash(s(i) \| E_{ki})$;

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 109
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

writing E_{ki}, H_{ni}, and H_{si} to the database;

said processor, via execution of the feedback module, generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

4. (Currently amended) The method of claim 3, said method comprising~~, as performed by the feedback module,~~ said processor, via execution of the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

5. (Original) The method of claim 4, wherein M=1.

6. (Original) The method of claim 4, wherein M>1.

7. (Original) A validation method for validating the N feedback entries resulting from performance of the method of claim 4, said validation method comprising verifying, by the vendor, an integrity of the N feedback entries received by the vendor as a result of said sending to the vendor: ((E_{ki}, H_{ni}), i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

8. (Currently amended) The validation method of claim 7, wherein said verifying comprises:

setting i = 0 and H(0) = n(0);

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 110
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

executing iterations i = 0, 1, …, N of a loop, wherein executing each iteration i of the loop comprises: setting H'_{ni} = Hash(H(i) || E_{ki}); determining [[if]] that $H'_{ni} = H_{ni}$ ~~is true~~; and ~~if $H'_{ni} = H_{ni}$ is determined to be true then~~ responsive to said determining that $H'_{ni} = H_{ni}$, setting H(i+1) = Hash(H(i)) and k(i+1) = Hash(k(i))~~, otherwise ascertaining that a first integrity failure has occurred~~;

~~if said executing the iterations has not determined that the first integrity failure has occurred then~~ after said executing:

decrypting E(k(N+1), n(N+1)) using key k(N+1) to infer n(N+1);

determining [[if]] that n(N+1) = H(N+1) ~~is true~~; and

~~if n(N+1) = H(N+1) has been determined to be true then~~ responsive to said determining that n(N+1) = H(N+1), ascertaining that the integrity of the N feedback entries received by the vendor has been verified~~, otherwise ascertaining that a second integrity failure has occurred~~.

9. (Currently amended) The validation method of claim 7, wherein the validation method further comprises, as performed by the vendor prior to said verifying:

calculating H'_{n0} = Hash(n(0) || E_{k0});

determining [[if]] that $H'_{n0} = H_{n0}$ ~~is true~~; and

~~if $H'_{ni} = H_{ni}$ is not determined to be true then ascertaining that an error has occurred, otherwise~~ responsive to said determining that $H'_{n0} = H_{n0}$, decrypting E_{ko} to infer FE(0) and recording that the database is set.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 111
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

10. (Original) A validation method for validating the N feedback entries resulting from performance of the method of claim 3, said validation method comprising verifying, by the user, an integrity of the N feedback entries in the database as a result of writing ((E_{ki}, H_{ni}, H_{si}), i= 1, …, N) to the database.

11. (Currently amended) The validation method of claim 10, wherein said verifying comprises:

setting i = 0 and S(0) = s(0);

executing iterations i = 0, 1, …, N of a loop, wherein executing each iteration i of the loop comprises: setting H'_{si} = Hash(S(i) || E_{ki}); determining [[if]] <u>that</u> $H'_{si} = H_{si}$ ~~is true~~; and ~~if $H'_{si} = H_{si}$ is determined to be true then~~ <u>responsive to said determining that $H'_{si} = H_{si}$,</u> setting S(i+1) = Hash(S(i))~~, otherwise ascertaining that a first integrity failure has occurred~~;

~~if said executing the iterations has not determined that the first integrity failure has occurred then~~ after said executing:

determining [[if]] <u>that</u> S(N+1) = s(N+1); and

~~if S(N+1) = s(N+1) has been determined to be true then~~ <u>responsive to said determining that S(N+1) = s(N+1),</u> ascertaining that the integrity of the N feedback entries in the database has been verified~~, otherwise ascertaining that a second integrity failure has occurred~~.

12. (Original) The method of claim 1, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, and wherein the method further comprises

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 112
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

permitting the feedback module to access the communication network, said permitting being controlled by the application firewall.

13. (Original) The method of claim 12, wherein the method further comprises preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

14. (Original) The method of claim 12, wherein the communication network comprises the Internet.

15. (Original) The method of claim 1, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

16. (Currently amended) A computer program product, comprising a computer ~~usable~~ readable storage medium having a computer readable program code ~~embodied~~ stored therein, execution of said computer readable program code ~~comprising an algorithm adapted~~ causing a processor to implement a method for processing feedback entries received from software, said software provided by a vendor to an end user machine~~, said end user machine comprising the software, a feedback module, and a database~~, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 113
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

parameter Y, and wherein said method comprises ~~comprising, as performed by the feedback module~~:

establishing ~~generating~~ a secret key k(0) ~~and~~ that is shared between a feedback module and the vendor and communicating ~~making~~ the key k(0) ~~known~~ to ~~both the vendor and~~ a user of the software;

establishing ~~generating~~ a secret key n(0) ~~and~~ that is shared between the feedback module and the vendor but not communicating ~~making~~ the key n(0) ~~known to the vendor but not~~ to the user;

said processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database;

said processor, via execution of the feedback module, generating a secret key s(0) and ~~making~~ communicating the key s(0) ~~known~~ to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of [[an]] the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$;

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that $H_{n0} = \text{Hash}(n(0) \| E_{k0})$;

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that $H_{s0} = \text{Hash}(s(0) \| E_{k0})$;

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 114
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

17. (Currently amended) The computer program product of claim 16, said method comprising~~, as performed by the feedback module~~:

said processor, via execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database.

18. (Currently amended) The computer program product of claim 17, said method comprising~~, as performed by the feedback module,~~ said processor, via execution of the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), …, FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, …, N comprising:

calculating parameters E_{ki}, H_{ni}, and H_{si} such that $E_{ki} = E(k(i), FE(i))$, $H_{ni} = Hash(n(i) \| E_{ki})$, and $H_{si} = Hash(s(i) \| E_{ki})$;

writing E_{ki}, H_{ni}, and H_{si} to the database;

generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

19. (Currently amended) The computer program product of claim 18, said method comprising~~, as performed by the feedback module,~~ said processor, via execution of the feedback module,

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 115
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

20. (Original) The computer program product of claim 19, wherein M=1.

21. (Original) The computer program product of claim 19, wherein M>1.

22. (Original) The computer program product of claim 16, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, and wherein the method further comprises permitting the feedback module to access the communication network, said permitting being controlled by the application firewall.

23. (Original) The computer program product of claim 22, wherein the method further comprises preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

24. (Original) The computer program product of claim 22, wherein the communication network comprises the Internet.

25. (Original) The computer program product of claim 16, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 116
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

software and a combination of the serial number of the software and the version number of the software.

26. (Currently amended) A process for deploying (or integrating) computing infrastructure, said process comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of performing a method for processing feedback entries received from software, said software provided by a vendor to an end user machine~~, said end user machine comprising the software, a feedback module, and a database~~, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, and wherein said method comprises ~~comprising, as performed by the feedback module~~:

~~module~~:

establishing ~~generating~~ a secret key k(0) ~~and~~ that is shared between a feedback module and the vendor and communicating ~~making~~ the key k(0) ~~known~~ to ~~both the vendor and~~ a user of the software;

establishing ~~generating~~ a secret key n(0) ~~and~~ that is shared between the feedback module and the vendor but not communicating ~~making~~ the key n(0) ~~known to the vendor but not~~ to the user;

a processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor, wherein the end user machine comprises the processor, the software, the feedback module, and a database;

said processor, via execution of the feedback module, generating a secret key s(0) and

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 117
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

~~making~~ communicating the key s(0) ~~known~~ to the user but not to the vendor;

said processor, via execution of the feedback module, generating an encryption E_{k0} of [[an]] the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$;

said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that $H_{n0} = Hash(n(0) \| E_{k0})$;

said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that $H_{s0} = Hash(s(0) \| E_{k0})$;

said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; and

said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor.

27. (Currently amended) The process of claim 26, said method comprising~~, as performed by the feedback module~~:

said processor, via execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database.

28. (Currently amended) The process of claim 27, said method comprising, ~~as performed by the feedback module,~~ said processor, via execution of the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), …, FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, …, N comprising:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 118
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

calculating parameters E_{ki}, H_{ni}, and H_{si} such that $E_{ki} = E(k(i), FE(i))$, $H_{ni} = Hash(n(i) \| E_{ki})$, and $H_{si} = Hash(s(i) \| E_{ki})$;

writing E_{ki}, H_{ni}, and H_{si} to the database;

generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

29. (Currently amended) The process of claim 28, said method comprising~~, as performed by the feedback module,~~ said processor, via execution of the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

30. (Original) The process of claim29, wherein M=1.

31. (Original) The process of claim 29, wherein M>1.

32. (Original) The process of claim 26, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, and wherein the method further comprises permitting the feedback module to access the communication network, said permitting being controlled by the application firewall.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 119
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

33. (Original) The process of claim 32, wherein the method further comprises preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

34. (Original) The process of claim 32, wherein the communication network comprises the Internet.

35. (Original) The process of claim 26, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 120
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

REMARKS

Applicant has amended claims 1-4, 8-9, 11, 16-19, and 26-29, and has cancelled claims 14, 24, and 34, during prosecution of this patent application. Applicant is not conceding in this patent application that the subject matter encompassed by said amended and cancelled claims are not patentable over the art cited by the Examiner, since the claim amendments and cancellations are only for facilitating expeditious prosecution of this patent application. Applicant respectfully reserves the right to pursue the subject matter encompassed by said amended and cancelled claims, and to pursue other claims, in one or more continuations and/or divisional patent applications.

Applicant has amended the drawings, the specification, and the claims without adding new matter as explained *infra*.

The Examiner rejected claims 1-35 under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter.

The Examiner rejected claims 1-35 under 35 U.S.C. § 112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner rejected claims 1, 12-16, 22-26 and 32-35 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) and further in view of Ginter, et al. (US Patent No. 5,892,900, hereinafter "Ginter").

The Examiner rejected claims 2-11, 17-21 and 27-31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal in view of Tsudik, in further view of Ginter and

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 121
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter "Wheeler").

Applicant next provides support for the amendment of the drawings, specification, and the claims, and also respectfully traverses the § 101, § 112 and § 103 rejections.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 122
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Support For the Amendment of the Drawings and Specification and Claimd

Applicant has amended the drawings and the specification without adding new matter.

Amendment of the Drawings

Step 55 in FIG. 5 has been amended to recite: "MAKE s(0) KNOWN TO USER" to correct a clerical error in the originally filed FIG. 5.

The amendment of step 55 in FIG. 5 is supported by the following text in the originally filed claim 1: "generating a secret key s(0) and making the key s(0) known to the user". The text "generating a secret key s(0)" is implemented in step 54 and the text "making the key s(0) known to the user" is implemented in the amended step 55 by reciting that the key s(0) is communicated to the user.

Amendment of the Specification

The paragraph beginning on page 12, line 17 includes the following amended text: "Step 51 generates the secret keys k(0) and n(0). Step 52 sends the generated secret keys k(0) and n(0) to the vendor 18 securely and communicates the secret key k(0) to the user 19 but does not communicate the secret key n(0) to the user 19", which is supported by the following text in the originally filed claim 1: "generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software; generating a secret key n(0) and making the key n(0) known to the vendor but not to the user".

The paragraph beginning on page 12, line 17 includes the following amended text: "Step 54 generates the secret key s(0) as a hash of the password P (i.e., as Hash(P)). Step 55 ~~sends k(0)~~

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 123
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

~~and n(0)~~ communicates the secret key s(0) to the ~~vendor 18 securely~~ user 19, but does not communicate the secret key s(0) to the vendor 18.", which is supported by the following text in the originally filed claim 1: "generating a secret key s(0) and making the key s(0) known to the user but not to the vendor".

Amendment of the Claims

Claims 1, 16, and 26 have been amended to include the following text: "establishing a secret key k(0) that is shared between a feedback module and the vendor and communicating the key k(0) to a user of the software", which is supported in the specification, page 11, lines 21-22 ("the feedback module 14 establishes two secret keys, namely k(0) and n(0), that are shared between the feedback module 14 and the vendor 18") and the following text in the originally filed claim 1: "generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software".

Claims 1, 16, and 26 have been amended to include the following text: "establishing a secret key n(0) that is shared between the feedback module and the vendor but not communicating the key n(0) to the user", which is supported in the specification, page 11, lines 21-22 ("the feedback module 14 establishes two secret keys, namely k(0) and n(0), that are shared between the feedback module 14 and the vendor 18") and the following text in the originally filed claim 1: "generating a secret key n(0) and making the key n(0) known to the vendor but not to the user".

Claims 1, 16, and 26 have been amended to include the following text: "a processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor", which is supported in the specification, page 11, lines 20-22 ("The

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 124
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

feedback module 14 also generates an identification tag, denoted illustratively as FBM_ID, that helps in uniquely identifying this installation of the software 13 with the vendor 18") and page 13, lines 10-11 ("the feedback module 14 sets parameter FE(0) equal to the identification tag denoted illustratively as FBM_ID").

Claims 1, 16, and 26 have been amended to include the following text: "said processor, via execution of the feedback module, generating a secret key s(0) and communicating the key s(0) to the user but not to the vendor", which is supported in the specification, page 12, lines 13-15 ("In step 42 of FIG. 4, the feedback module 14 generates a secret key s(0) for use between the user 19 and the feedback module 14. The feedback module 14 discloses the secret key s(0) to the user 19.") and the following text in the originally filed claim 1: "generating a secret key s(0) and making the key s(0) known to the user but not to the vendor".

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 125
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 101: Claims 1-35

The Examiner rejected claims 1-35 under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter.

The Examiner argues that independent claims 1 and 26 fail to meet the test for statutory subject matter under 35 U.S.C. § 101 as set forth in *In re Bilski*, 545 F.3d 943 (Fed. Cir. 2008) (en banc).

In response, claim 1 and 26 have been amended to recite individual steps being performed by a particular machine, namely a processor of an end user machine, in compliance with the machine prong of the machine-or-transformation test set forth by the Federal Circuit in *In re Bilski*, 545 F.3d 943 (Fed. Cir. 2008) (en banc).

The Examiner argues that independent claims 1, 16, and 26 describe a purely abstract process, namely "a process consisting solely of mathematical operations, i.e., converting one set of numbers into another set of numbers".

In response, Applicant respectfully points out that claims 1 and 26 do not recite a purely abstract process, because claims 1 and 26 recite a tangible result in the steps of "sending E_{k0}, H_{n0}, and H_{s0} to the database; and ... sending E_{k0} and H_{n0} to the vendor" which do not include "mathematical operations, i.e., converting one set of numbers into another set of numbers".

With respect to claim 16, the Examiner argues: "Claim 16 recites "A computer program product, comprising a computer usable medium having a computer readable program code embodied therein. However, this is merely software, and it has been held that software without a

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 126
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

required computer-readable medium storing software that, *when executed,* causes the computer to perform a particular process or method (MPEP 2106.01) is merely nonfunctional descriptive material and non-statutory under 35 U.S.C. 101."

In response, Applicant has amended claim 16 as follows: "A computer program product, comprising a computer ~~usable~~ readable storage medium having a computer readable program code ~~embodied~~ stored therein, execution of said computer readable program code ~~comprising an algorithm adapted~~ causing a processor to implement a method for ...", which recites that computer readable program code is stored on a computer readable storage medium and that execution of the program code causes a processor to implement a method.

Based on the preceding arguments, Applicant respectfully requests that the rejection of claims 1-35 under 35 U.S.C. § 101 be withdrawn.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 127
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 112, Second Paragraph: Claims 1-35

The Examiner rejected claims 1-35 under 35 U.S.C. § 112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner argues: "Claims 1, 16, and 26 recite "...making the key n(0) known to the vendor but not to the user..." However, the claims also previously recite "...said end user machine comprising the software, *a feedback module,* and a database... said method comprising ,as performed by the *feedback module...* " Thus, the claim recites that the steps of the method, including the step of "...generating a secret key n(0)..." are performed by a feedback module on the end user machine. It is unclear to one of ordinary skill how the secret key n(0) is not known to the user when it is generated by the end user machine."

In response, Applicant asserts that the pertinent feature in claims 1, 16, and 26 is "establishing a secret key n(0) that is shared between the feedback module and the vendor but not communicating the key n(0) to the user". Applicants assert that the specification does not disclose that the user has access to n(0). Furthermore, even if the user has access to n(0), the specification does not disclose that the user has actually accessed n(0). Therefore, it is clear that the limitation of "establishing a secret key n(0) that is shared between the feedback module and the vendor" is not inconsistent with the secret key n(0) not being communicated to the user.

The Examiner argues: "The claims further recite "...generating a parameter Hn0 such that Hn0 = Hash(n(0) || Ek0)..." It is unclear to one of ordinary skill how the feedback module in the user computer can use n(0) when is only known to the vendor."

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 128
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In response, Applicant asserts that claims 1, 16, and 26 do not recite that n(0) is only known to the vendor, but rather recite "establishing a secret key n(0) that is shared between the feedback module and the vendor". Therefore, the feedback module has access to n(0) and can use n(0) to generate H_{n0} via $H_{n0} = \text{Hash}(n(0) \| E_{k0}$ as claimed.

The Examiner argues: "Claims 1, 16, and 26 also recite "...making the key...known..." However, it is unclear what action "...making the key...known..." comprises."

In response, Applicant asserts that the preceding issue can be framed as: after K is generated, how can K be communicated to X? The answer is that K may be communicated to X by any method known to a person of ordinary skill in the art of computer programming. For example, K may be sent to X (e.g., see specification, page 12, lines 19-20: "sends the generated secret keys k(0) and n(0) to the vendor 18"). As another example, K may be displayed K to X (e.g., see specification, page 20, lines 19-20: "The output device 93 displays output from the computer code 97"). The scope of claims 1, 16, and 26 encompasses all of such methods (for communicated K to X) known to a person of ordinary skill in the art of computer programming and is not limited to any specific method of such known methods.

The Examiner argues: "Claims 1, 16, and 26 recite the limitation "...an identification tag FE(0)...". However, claims 3, 18, and 28 recite the limitation "...said N feedback entries denoted as FE(1), ..., FE(N)..." It is unclear to one of ordinary skill the whether series of data denoted by "FE" consists of identification tags or feedback entries."

In response, Applicant asserts that the specification, page 13, line 10 assigns the label "identification tag" to FE(0), and the specification does not assign any other label to FE(0).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 129
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In further response, Applicant asserts that the specification, page 14, lines 14-15 assigns the label "feedback entry" to FE(i) such that the first such feedback entry is for i = 1. The specification, page 15, lines 13-15 states that there are N such feedback entries FE(1), FE(2), ... , FE(N). There is no text anywhere in the specification that labels FE(0) as a feedback entry or that labels as FE(1), ..., FE(N) as identifcation tags.

Therefore, it is clear that FE(0) is an identification tag and FE(1), FE(2), ..., FE(N) are feedback entries.

Based on the preceding arguments, Applicant respectfully requests that the rejection of claims 1-35 under 35 U.S.C. § 112, second paragraph be withdrawn.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 130
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 103(a): Claims 1, 12-16, 22-26 and 32-35

The Examiner rejected claims 1, 12-16, 22-26 and 32-35 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) and further in view of Ginter, et al. (US Patent No. 5,892,900, hereinafter "Ginter").

Applicant respectfully contends that claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter, because Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest each and every feature of 1, 16, and 26.

A first example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "establishing a secret key k(0) that is shared between a feedback module and the vendor and communicating the key k(0) to a user of the software".

The Examiner argues: "Elgamal discloses ... generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software (Elgamal **2:1-15; 7:41-51; 8:5-20; 33:9-13)**".

In response, Applicant notes that the Examiner is arguing that the claimed secret key k(0) is represented in Elgamal as a master key that is shared between the client and the server, which is explained in the Examiner's citation of Elgamal, col. 7, lines 41-51. However, Elgamel does not disclose that the master key has been communicated to a user at the client machine, as required by the preceding feature of claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 131
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A second example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "establishing a secret key n(0) that is shared between the feedback module and the vendor but not communicating the key n(0) to the user".

The Examiner argues: "Elgamal discloses ... generating a key by the user terminal that is used for encryption by the vendor (Elgamal **23:9-19; 28:38-40; 33:1-4)**".

In response, Applicant respectfully contends that the Examiner is arguing that the claimed secret key n(0) is represented in Elgamal as a client session key that is generated by the client and a server session key that is generated by the server, both the client session key and the server session key being generated from the master key that is shared between the client and the server, which is explained in the Examiner's citation of Elgamal, col. 23, lines 9-19.

Thus, the client session key and the server session key are distinct keys that are separately generated by the client and the server, respectively, and are thus not shared between the client and the server as required by the preceding feature of claims 1, 16, and 26.

Furthermore, Elgamal does not disclose that the client session key is not communicated to a user of the client machine, as required by the preceding feature of claims 1, 16, and 26.

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 132
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

A third example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "generating an identification tag FE(0) that identifies the software with the vendor".

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A fourth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "generating a secret key s(0) and communicating the key s(0) to the user but not to the vendor".

The Examiner argues:

"Tsudik in view of Elgamal does not specifically disclose generating a key known only to the user or that the encrypted data is stored at the client... Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database (Ginter **222:50-61).** Ginter further discloses storage of authentication values (Ginter 245:55-62; 246:18-23, 27-50)... Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal to use the secret prefix method of generating a message authentication code in order to produce unforgeable integrity values ***without using encryption*** so as to provide increased speed by minimizing the use of encryption software (Tsudik pp. **30-31** Motivation). Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik to include the user generating a secure database key known only to the PPE and storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter **222:55-57).**" (emphasis added).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 133
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In response, Applicant respectfully contends that Ginter does not disclose that secret key s(0) is communicated to the user, as required by preceding feature of claims 1, 16, and 26.

In further response, Applicant respectfully contends that the Examiner's reasons as to why it is allegedly obvious to modify Elgamal by incorporating the preceding feature of claims 1, 16, and 26 into Elgamal is not persuasive.

A first reason why the Examiner's suggested modification Elgamal is not persuasive is that the Examiner's argument depends on a PPE. However, Ginter does not explain the meaning of "PPE" and Applicants do not know what a PPE is in Ginter. If the Examiner knows what the intended meaning of PPE is in Ginter, then the Examiner should explain and prove what the intended meaning of PPE is in Ginter. In the absence of knowledge of what a PPE is, Applicant respectfully contends that the Examiner's argument cannot be reasonably understood, is accordingly ambiguous, and thus not persuasive.

A second reason why the Examiner's suggested modification Elgamal is not persuasive is that the Examiner's argument asserts that modifying Elgamal in conjunction with the preceding feature of claims 1, 16, and 26 enables the use of encryption to be avoided. However, the use of encryption is within the essence of Elgamal's invention (see Elgamal, abstract and claim 1). Therefore, the Examiner's argument, which results in not using encryption in conjunction with the preceding feature of claims 1, 16, and 26, is not persuasive.

A third reason why the Examiner's suggested modification Elgamal is not persuasive is that the Examiner's argument is specific to the use of databases. However, Elgamal's invention does not relate to the use of a database. Therefore, the Examiner's suggested modification of Elgamal has no relevance to Elgamal's invention and is thus not persuasive.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 134
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A fifth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$".

The Examiner argues: "Elgamal discloses ... encrypting information to be transferred to the vendor (Elgamal **2:5-10; 7:2-8; 8:9-11; 7:62-8:4; 13:17-28; 14:65-68)**".

In response, Applicant asserts that the preceding feature of claims 1, 16, and 26 requires that the identification tag FE(0) be encrypted and, although Elgamal discloses encrypting information, Elgamal does not disclose encrypting the identification tag FE(0) that identifies the software with the vendor, as required by the preceding feature of claims 1, 16, and 26.

In further response, Applicant asserts that the preceding feature of claims 1, 16, and 26 requires that FE(0) be encrypted through use of the secret key k(0). However, the Examiner alleges that the secret key k(0) is represented in Elgamal by the master key as discussed *supra* and Elgamal does not disclose that the encryption of information in Elgamal is performed through use of the master key. To the contrary, Elgamal discloses that the encryption of information in Elgamal is performed through use of session keys which are generated from the master key (Elgamal, col. 7, lines 43-46 and col. 23, lines 9-12).

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 135
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

A sixth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that H_{n0} = Hash(n(0) || E_{k0}); said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that H_{s0} = Hash(s(0) || E_{k0})".

The Examiner argues:

"Elgamal further discloses the use of a MAC (message authentication code) to verify the integrity of data that is to be transmitted and that the MAC includes a hash of the data and a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27)**.... Tsudik discloses the use of the secret prefix method of generating a MAC using ahash function. Tsudik discloses that in this method, two principals agree on a secret, S_ab for example, and when A sends a message M to B, it generates an MD4 hash of S_ab concatenated to the beginning of the message such that HashValue = MD4Hash(S_ab || M). The receiver would then use its knowledge of S_ab and the received message to recompute the hash value and compare it to the received hash value to verify the integrity of the message (Tsudik p. **32,** Protocol Description; pp. **33-34** Secret Prefix)."

In response, Applicants assert that, if the keys n(0) and s(0) are used as the "secret" in Elgamal and the "secret prefix" in Tsudick, then the preceding feature of claims 1, 16, and 26 requires that E_{k0} be the "data" or "message" to be transmitted. However, Elgamal does not disclose transmitting E_{k0}. In fact, there is no disclosure in Elgamal, Tsudik, or Ginter of the existence of E_{k0}, namely an encryption of the identification tag (that that identifies the software with the vendor) using the key k(0).

In further response, Applicant asserts that Tsudik's method requires that, in application to the client and server in Elgamal, the client must communicate the secret prefix (i.e., n(0) and

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 136
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

s(*0) in claims 1, 16, 26) to the server in secret (see Tsudik, page 32, lines 10-13). However, claims 1, 16, and 26 recite that the key s(0) is not communicated to the vendor (i.e., the server in Elgamal). Therefore, it is logically impossible to satisfy the requirement of the key s(0) not being communicated to the vendor if Tsudik's "secret prefix" method is used to modify Elgamal.

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A seventh example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor".

The Examiner argues: "Ginter further discloses storage of authentication values (Ginter **245:55-62; 246:18-23, 27-50)**... Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik to include ... storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter **222:55-57)**.".

In response, it is not clear that storing E_{k0}, H_{n0},and H_{s0} in the user's database would protect data in the user's database from be accessed by another party as alleged by the Examiner in support of modifying Elgamal in view of Tsudik by storing E_{k0}, H_{n0},and H_{s0} in the user's database.

In further response and assuming that storing E_{k0}, H_{n0},and H_{s0} in the user's database would protect data in the user's database from be accessed by another party (for the sake of

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 137
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

argument only), Applicants assert that the Examiner's reason for modifying Elgamal in view of Tsudik to store E_{k0} and H_{n0} in the user's database ("to be able to securely store data that cannot be accessed by another party in a database at the user's device) is negated by the claimed limitation. "sending E_{k0} and H_{n0} to the vendor" which would enable the vendor to access the very data in the user's device that is intended to be protected from such access by storing E_{k0} and H_{n0} in the user's database in the first place.

Thus, the Examiner's argument is not persuasive.

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

Based on the preceding arguments, Applicant respectfully maintains that claim 1 is not unpatentable over Elgamal in view of Tsudik and further in view of Ginter, and that claim 1 is in condition for allowance. Since claims 12-15 depend from claim 1, Applicant contends that claims 12-15 are likewise in condition for allowance. Since claims 22-25 depend from claim 16, Applicant contends that claims 22-25 are likewise in condition for allowance. Since claims 32-35 depend from claim 26, Applicant contends that claims 32-35 are likewise in condition for allowance.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 138
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 103(a): Claims 2-11, 17-21 and 27-31

The Examiner rejected claims 2-11, 17-21 and 27-31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter "Wheeler").

Since claims 2-11 depend from claim 1, which Applicants have argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter under 35 U.S.C. §103(a), Applicants maintain that claims 2-11 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler under 35 U.S.C. §103(a).

Since claims 17-21 depend from claim 16, which Applicants have argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter under 35 U.S.C. §103(a), Applicants maintain that claims 17-21 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler under 35 U.S.C. §103(a).

Since claims 27-21 depend from claim 26, which Applicants have argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter under 35 U.S.C. §103(a), Applicants maintain that claims 27-31 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler under 35 U.S.C. §103(a).

In addition with respect to claims 2, 17, and 27, Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler does not disclose the feature: "said processor, via

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 139
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database"

The Examiner argues:

"Elgamal in view of Tsudik in further view of Ginter does not specifically disclosegenerating a series of keys in which a new key is generated by hashing the last key and using the keys to generate a series of hash values... Wheeler discloses computing a series of keys used to encrypt blocks of data andgenerate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68)...** Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to include computing a series of keys used ***to encrypt blocks of data*** as disclosed in Wheeler in order to allow the data to be transferred using broadcast transmission (Wheeler Paragraph **53)**" (emphasis added).

In response, Applicants note that the Examiner cites Wheeler for modifying Elgamal "***to encrypt blocks of data***". Yet, the Examiner cites Tsudik "to use the secret prefix method ... ***without using encryption***". Thus, the Examiner's reliance on Wheeler is inconsistent with the Examiner's reliance on Tsudik.

Accordingly, Applicant respectfully contends that the preceding argument by the Examiner is not persuasive.

Therefore, claims 2, 17, and 27 likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 140
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

CONCLUSION

Based on the preceding arguments, Applicant respectfully believes that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicant invites the Examiner to contact Applicant's representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account 09-0457 (IBM).

Date: 06/30/2009

Jack P. Friedman
Registration No. 44,688

Customer No. 30449
Schmeiser, Olsen & Watts
22 Century Hill Drive - Suite 302
Latham, New York 12110
Telephone (518) 220-1850
Facsimile (518) 220-1857
Email: jfriedman@iplawusa.com

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 141
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

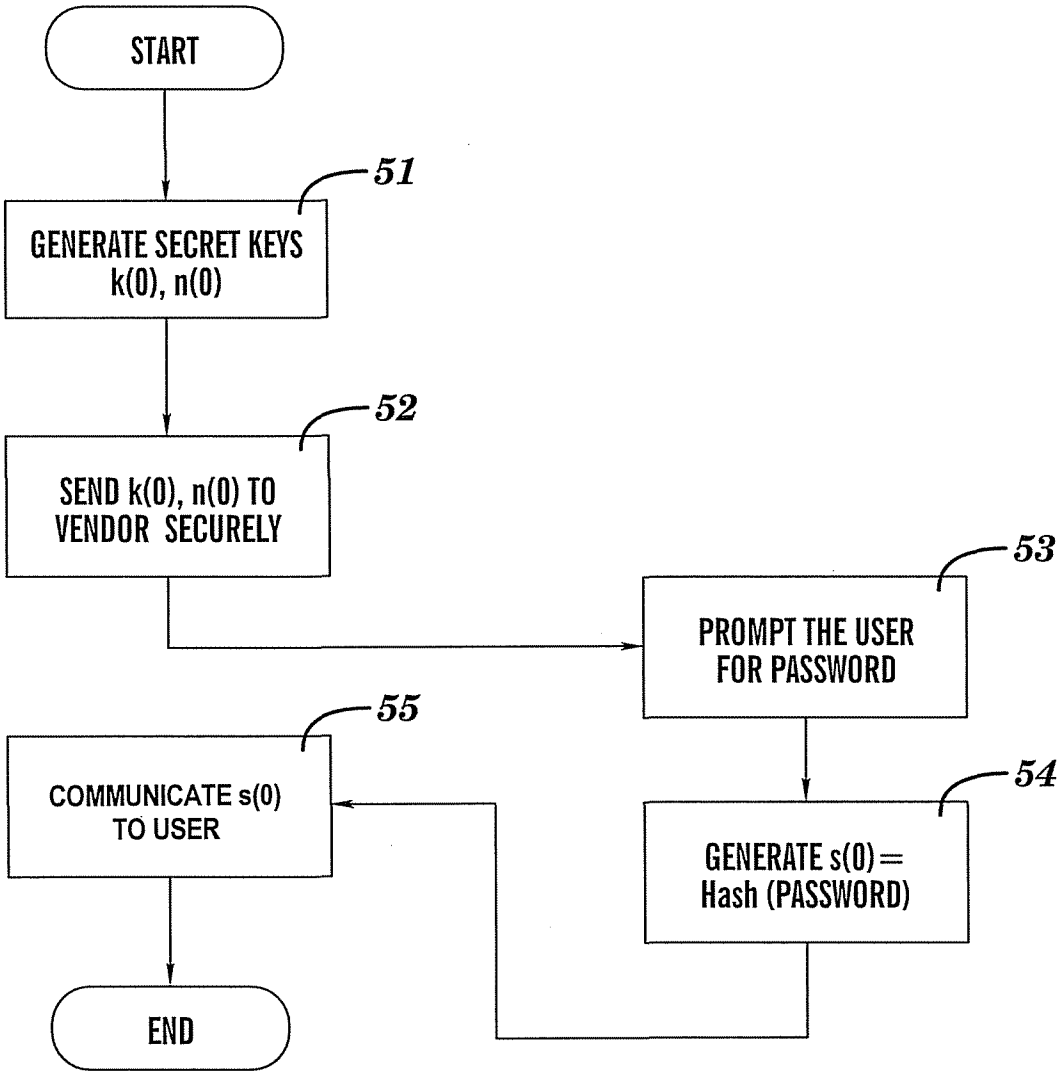
START
51
GENERATE SECRET KEYS k(0), n(0)
52
SEND k(0), n(0) TO VENDOR SECURELY
53
PROMPT THE USER FOR PASSWORD
54
GENERATE s(0) = Hash (PASSWORD)
55
COMMUNICATE s(0) TO USER
END

FIG. 5

Electronic Acknowledgement Receipt

EFS ID:	5622294
Application Number:	11325719
International Application Number:	
Confirmation Number:	7235
Title of Invention:	System and method for processing feedback entries received from software
First Named Inventor/Applicant Name:	Vijil Enara Chenthamarakshan
Customer Number:	30449
Filer:	Jack P. Friedman/Kimberly Dwileski
Filer Authorized By:	Jack P. Friedman
Attorney Docket Number:	IN920050028US1
Receipt Date:	01-JUL-2009
Filing Date:	05-JAN-2006
Time Stamp:	09:16:23
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	Amendment/Req. Reconsideration-After Non-Final Reject	IN920050028US1-amendment.pdf	2945203 b0843587ecacbe17331d77d89ffa189b0856e3a9	no	37

Warnings:

Information:

2	Drawings-other than black and white line drawings	IN920050028US1-ReplacementSheet.pdf	42572 ab3950f09a2398c5e80fb2daaff390158ee143e1	no	1

Warnings:

Information:

Total Files Size (in bytes):	2987775

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.

REMARKS

Applicant has amended claims 1-4, 8-9, 11, 16-19, and 26-29, and has cancelled claims 14, 24, and 34, during prosecution of this patent application. Applicant is not conceding in this patent application that the subject matter encompassed by said amended and cancelled claims are not patentable over the art cited by the Examiner, since the claim amendments and cancellations are only for facilitating expeditious prosecution of this patent application. Applicant respectfully reserves the right to pursue the subject matter encompassed by said amended and cancelled claims, and to pursue other claims, in one or more continuations and/or divisional patent applications.

Applicant has amended the drawings, the specification, and the claims without adding new matter as explained *infra*.

The Examiner rejected claims 1-35 under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter.

The Examiner rejected claims 1-35 under 35 U.S.C. § 112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner rejected claims 1, 12-16, 22-26 and 32-35 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) and further in view of Ginter, et al. (US Patent No. 5,892,900, hereinafter "Ginter").

The Examiner rejected claims 2-11, 17-21 and 27-31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal in view of Tsudik, in further view of Ginter and

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 145
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter "Wheeler").

Applicant next provides support for the amendment of the drawings, specification, and the claims, and also respectfully traverses the § 101, § 112 and § 103 rejections.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 146
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Support For the Amendment of the Drawings and Specification and Claimd

Applicant has amended the drawings and the specification without adding new matter.

Amendment of the Drawings

Step 55 in FIG. 5 has been amended to recite: "MAKE s(0) KNOWN TO USER" to correct a clerical error in the originally filed FIG. 5.

The amendment of step 55 in FIG. 5 is supported by the following text in the originally filed claim 1: "generating a secret key s(0) and making the key s(0) known to the user". The text "generating a secret key s(0)" is implemented in step 54 and the text "making the key s(0) known to the user" is implemented in the amended step 55 by reciting that the key s(0) is communicated to the user.

Amendment of the Specification

The paragraph beginning on page 12, line 17 includes the following amended text: "Step 51 generates the secret keys k(0) and n(0). Step 52 sends the generated secret keys k(0) and n(0) to the vendor 18 securely and communicates the secret key k(0) to the user 19 but does not communicate the secret key n(0) to the user 19", which is supported by the following text in the originally filed claim 1: "generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software; generating a secret key n(0) and making the key n(0) known to the vendor but not to the user".

The paragraph beginning on page 12, line 17 includes the following amended text: "Step 54 generates the secret key s(0) as a hash of the password P (i.e., as Hash(P)). Step 55 ~~sends k(0)~~

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 147
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

~~and n(0)~~ communicates the secret key s(0) to the ~~vendor 18 securely~~ user 19, but does not communicate the secret key s(0) to the vendor 18.", which is supported by the following text in the originally filed claim 1: "generating a secret key s(0) and making the key s(0) known to the user but not to the vendor".

Amendment of the Claims

Claims 1, 16, and 26 have been amended to include the following text: "establishing a secret key k(0) that is shared between a feedback module and the vendor and communicating the key k(0) to a user of the software", which is supported in the specification, page 11, lines 21-22 ("the feedback module 14 establishes two secret keys, namely k(0) and n(0), that are shared between the feedback module 14 and the vendor 18") and the following text in the originally filed claim 1: "generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software".

Claims 1, 16, and 26 have been amended to include the following text: "establishing a secret key n(0) that is shared between the feedback module and the vendor but not communicating the key n(0) to the user", which is supported in the specification, page 11, lines 21-22 ("the feedback module 14 establishes two secret keys, namely k(0) and n(0), that are shared between the feedback module 14 and the vendor 18") and the following text in the originally filed claim 1: "generating a secret key n(0) and making the key n(0) known to the vendor but not to the user".

Claims 1, 16, and 26 have been amended to include the following text: "a processor, via execution of a feedback module, generating an identification tag FE(0) that identifies the software with the vendor", which is supported in the specification, page 11, lines 20-22 ("The

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 148
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

feedback module 14 also generates an identification tag, denoted illustratively as FBM_ID, that helps in uniquely identifying this installation of the software 13 with the vendor 18") and page 13, lines 10-11 ("the feedback module 14 sets parameter FE(0) equal to the identification tag denoted illustratively as FBM_ID").

Claims 1, 16, and 26 have been amended to include the following text: "said processor, via execution of the feedback module, generating a secret key s(0) and communicating the key s(0) to the user but not to the vendor", which is supported in the specification, page 12, lines 13-15 ("In step 42 of FIG. 4, the feedback module 14 generates a secret key s(0) for use between the user 19 and the feedback module 14. The feedback module 14 discloses the secret key s(0) to the user 19.") and the following text in the originally filed claim 1: "generating a secret key s(0) and making the key s(0) known to the user but not to the vendor".

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 149
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 101: Claims 1-35

The Examiner rejected claims 1-35 under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter.

The Examiner argues that independent claims 1 and 26 fail to meet the test for statutory subject matter under 35 U.S.C. § 101 as set forth in *In re Bilski*, 545 F.3d 943 (Fed. Cir. 2008) (en banc).

In response, claim 1 and 26 have been amended to recite individual steps being performed by a particular machine, namely a processor of an end user machine, in compliance with the machine prong of the machine-or-transformation test set forth by the Federal Circuit in *In re Bilski*, 545 F.3d 943 (Fed. Cir. 2008) (en banc).

The Examiner argues that independent claims 1, 16, and 26 describe a purely abstract process, namely "a process consisting solely of mathematical operations, i.e., converting one set of numbers into another set of numbers".

In response, Applicant respectfully points out that claims 1 and 26 do not recite a purely abstract process, because claims 1 and 26 recite a tangible result in the steps of "sending E_{k0}, H_{n0}, and H_{s0} to the database; and ... sending E_{k0} and H_{n0} to the vendor" which do not include "mathematical operations, i.e., converting one set of numbers into another set of numbers".

With respect to claim 16, the Examiner argues: "Claim 16 recites "A computer program product, comprising a computer usable medium having a computer readable program code embodied therein. However, this is merely software, and it has been held that software without a

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 150
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

required computer-readable medium storing software that, *when executed,* causes the computer to perform a particular process or method (MPEP 2106.01) is merely nonfunctional descriptive material and non-statutory under 35 U.S.C. 101."

In response, Applicant has amended claim 16 as follows: "A computer program product, comprising a computer ~~usable~~ readable storage medium having a computer readable program code ~~embodied~~ stored therein, execution of said computer readable program code ~~comprising an algorithm adapted~~ causing a processor to implement a method for ...", which recites that computer readable program code is stored on a computer readable storage medium and that execution of the program code causes a processor to implement a method.

Based on the preceding arguments, Applicant respectfully requests that the rejection of claims 1-35 under 35 U.S.C. § 101 be withdrawn.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 151
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 112, Second Paragraph: Claims 1-35

The Examiner rejected claims 1-35 under 35 U.S.C. § 112, second paragraph, as being indefinite for allegedly failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner argues: "Claims 1, 16, and 26 recite "...making the key n(0) known to the vendor but not to the user..." However, the claims also previously recite "...said end user machine comprising the software, *a feedback module,* and a database... said method comprising ,as performed by the *feedback module...* " Thus, the claim recites that the steps of the method, including the step of "...generating a secret key n(0)..." are performed by a feedback module on the end user machine. It is unclear to one of ordinary skill how the secret key n(0) is not known to the user when it is generated by the end user machine."

In response, Applicant asserts that the pertinent feature in claims 1, 16, and 26 is "establishing a secret key n(0) that is shared between the feedback module and the vendor but not communicating the key n(0) to the user". Applicants assert that the specification does not disclose that the user has access to n(0). Furthermore, even if the user has access to n(0), the specification does not disclose that the user has actually accessed n(0). Therefore, it is clear that the limitation of "establishing a secret key n(0) that is shared between the feedback module and the vendor" is not inconsistent with the secret key n(0) not being communicated to the user.

The Examiner argues: "The claims further recite "...generating a parameter Hn0 such that Hn0 = Hash(n(0) || Ek0)..." It is unclear to one of ordinary skill how the feedback module in the user computer can use n(0) when is only known to the vendor."

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 152
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In response, Applicant asserts that claims 1, 16, and 26 do not recite that n(0) is only known to the vendor, but rather recite "establishing a secret key n(0) that is shared between the feedback module and the vendor". Therefore, the feedback module has access to n(0) and can use n(0) to generate H_{n0} via $H_{n0} = \text{Hash}(n(0) \| E_{k0}$ as claimed.

The Examiner argues: "Claims 1, 16, and 26 also recite "...making the key...known..." However, it is unclear what action "...making the key...known..." comprises."

In response, Applicant asserts that the preceding issue can be framed as: after K is generated, how can K be communicated to X? The answer is that K may be communicated to X by any method known to a person of ordinary skill in the art of computer programming. For example, K may be sent to X (e.g., see specification, page 12, lines 19-20: "sends the generated secret keys k(0) and n(0) to the vendor 18"). As another example, K may be displayed K to X (e.g., see specification, page 20, lines 19-20: "The output device 93 displays output from the computer code 97"). The scope of claims 1, 16, and 26 encompasses all of such methods (for communicated K to X) known to a person of ordinary skill in the art of computer programming and is not limited to any specific method of such known methods.

The Examiner argues: "Claims 1, 16, and 26 recite the limitation "...an identification tag FE(0)...". However, claims 3, 18, and 28 recite the limitation "...said N feedback entries denoted as FE(1), ..., FE(N)..." It is unclear to one of ordinary skill the whether series of data denoted by "FE" consists of identification tags or feedback entries."

In response, Applicant asserts that the specification, page 13, line 10 assigns the label "identification tag" to FE(0), and the specification does not assign any other label to FE(0).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 153
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In further response, Applicant asserts that the specification, page 14, lines 14-15 assigns the label "feedback entry" to FE(i) such that the first such feedback entry is for i = 1. The specification, page 15, lines 13-15 states that there are N such feedback entries FE(1), FE(2), ... , FE(N). There is no text anywhere in the specification that labels FE(0) as a feedback entry or that labels as FE(1), ..., FE(N) as identifcation tags.

Therefore, it is clear that FE(0) is an identification tag and FE(1), FE(2), ..., FE(N) are feedback entries.

Based on the preceding arguments, Applicant respectfully requests that the rejection of claims 1-35 under 35 U.S.C. § 112, second paragraph be withdrawn.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 154
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 103(a): Claims 1, 12-16, 22-26 and 32-35

The Examiner rejected claims 1, 12-16, 22-26 and 32-35 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) and further in view of Ginter, et al. (US Patent No. 5,892,900, hereinafter "Ginter").

Applicant respectfully contends that claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter, because Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest each and every feature of 1, 16, and 26.

A first example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "establishing a secret key k(0) that is shared between a feedback module and the vendor and communicating the key k(0) to a user of the software".

The Examiner argues: "Elgamal discloses ... generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software (Elgamal **2:1-15; 7:41-51; 8:5-20; 33:9-13)**".

In response, Applicant notes that the Examiner is arguing that the claimed secret key k(0) is represented in Elgamal as a master key that is shared between the client and the server, which is explained in the Examiner's citation of Elgamal, col. 7, lines 41-51. However, Elgamel does not disclose that the master key has been communicated to a user at the client machine, as required by the preceding feature of claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 155
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A second example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "establishing a secret key n(0) that is shared between the feedback module and the vendor but not communicating the key n(0) to the user".

The Examiner argues: "Elgamal discloses ... generating a key by the user terminal that is used for encryption by the vendor (Elgamal **23:9-19; 28:38-40; 33:1-4)**".

In response, Applicant respectfully contends that the Examiner is arguing that the claimed secret key n(0) is represented in Elgamal as a client session key that is generated by the client and a server session key that is generated by the server, both the client session key and the server session key being generated from the master key that is shared between the client and the server, which is explained in the Examiner's citation of Elgamal, col. 23, lines 9-19.

Thus, the client session key and the server session key are distinct keys that are separately generated by the client and the server, respectively, and are thus not shared between the client and the server as required by the preceding feature of claims 1, 16, and 26.

Furthermore, Elgamal does not disclose that the client session key is not communicated to a user of the client machine, as required by the preceding feature of claims 1, 16, and 26.

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 156
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

A third example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "generating an identification tag FE(0) that identifies the software with the vendor".

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A fourth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "generating a secret key s(0) and communicating the key s(0) to the user but not to the vendor".

The Examiner argues:

"Tsudik in view of Elgamal does not specifically disclose generating a key known only to the user or that the encrypted data is stored at the client... Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database (Ginter **222:50-61).** Ginter further discloses storage of authentication values (Ginter 245:55-62; 246:18-23, 27-50)... Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal to use the secret prefix method of generating a message authentication code in order to produce unforgeable integrity values ***without using encryption*** so as to provide increased speed by minimizing the use of encryption software (Tsudik pp. **30-31** Motivation). Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik to include the user generating a secure database key known only to the PPE and storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter **222:55-57).**" (emphasis added).

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 157
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In response, Applicant respectfully contends that Ginter does not disclose that secret key s(0) is communicated to the user, as required by preceding feature of claims 1, 16, and 26.

In further response, Applicant respectfully contends that the Examiner's reasons as to why it is allegedly obvious to modify Elgamal by incorporating the preceding feature of claims 1, 16, and 26 into Elgamal is not persuasive.

A first reason why the Examiner's suggested modification Elgamal is not persuasive is that the Examiner's argument depends on a PPE. However, Ginter does not explain the meaning of "PPE" and Applicants do not know what a PPE is in Ginter. If the Examiner knows what the intended meaning of PPE is in Ginter, then the Examiner should explain and prove what the intended meaning of PPE is in Ginter. In the absence of knowledge of what a PPE is, Applicant respectfully contends that the Examiner's argument cannot be reasonably understood, is accordingly ambiguous, and thus not persuasive.

A second reason why the Examiner's suggested modification Elgamal is not persuasive is that the Examiner's argument asserts that modifying Elgamal in conjunction with the preceding feature of claims 1, 16, and 26 enables the use of encryption to be avoided. However, the use of encryption is within the essence of Elgamal's invention (see Elgamal, abstract and claim 1). Therefore, the Examiner's argument, which results in not using encryption in conjunction with the preceding feature of claims 1, 16, and 26, is not persuasive.

A third reason why the Examiner's suggested modification Elgamal is not persuasive is that the Examiner's argument is specific to the use of databases. However, Elgamal's invention does not relate to the use of a database. Therefore, the Examiner's suggested modification of Elgamal has no relevance to Elgamal's invention and is thus not persuasive.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 158
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A fifth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "said processor, via execution of the feedback module, generating an encryption E_{k0} of the identification tag FE(0) using the secret key k(0) such that $E_{k0} = E(k(0),FE(0))$".

The Examiner argues: "Elgamal discloses ... encrypting information to be transferred to the vendor (Elgamal **2:5-10; 7:2-8; 8:9-11; 7:62-8:4; 13:17-28; 14:65-68)**".

In response, Applicant asserts that the preceding feature of claims 1, 16, and 26 requires that the identification tag FE(0) be encrypted and, although Elgamal discloses encrypting information, Elgamal does not disclose encrypting the identification tag FE(0) that identifies the software with the vendor, as required by the preceding feature of claims 1, 16, and 26.

In further response, Applicant asserts that the preceding feature of claims 1, 16, and 26 requires that FE(0) be encrypted through use of the secret key k(0). However, the Examiner alleges that the secret key k(0) is represented in Elgamal by the master key as discussed *supra* and Elgamal does not disclose that the encryption of information in Elgamal is performed through use of the master key. To the contrary, Elgamal discloses that the encryption of information in Elgamal is performed through use of session keys which are generated from the master key (Elgamal, col. 7, lines 43-46 and col. 23, lines 9-12).

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 159
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

A sixth example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "said processor, via execution of the feedback module, generating a parameter H_{n0} using the secret key n(0) such that H_{n0} = Hash(n(0) || E_{k0}); said processor, via execution of the feedback module, generating a parameter H_{s0} using the secret key s(0) such that H_{s0} = Hash(s(0) || E_{k0})".

The Examiner argues:

"Elgamal further discloses the use of a MAC (message authentication code) to verify the integrity of data that is to be transmitted and that the MAC includes a hash of the data and a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27)**.... Tsudik discloses the use of the secret prefix method of generating a MAC using ahash function. Tsudik discloses that in this method, two principals agree on a secret, S_ab for example, and when A sends a message M to B, it generates an MD4 hash of S_ab concatenated to the beginning of the message such that HashValue = MD4Hash(S_ab || M). The receiver would then use its knowledge of S_ab and the received message to recompute the hash value and compare it to the received hash value to verify the integrity of the message (Tsudik p. **32,** Protocol Description; pp. **33-34** Secret Prefix)."

In response, Applicants assert that, if the keys n(0) and s(0) are used as the "secret" in Elgamal and the "secret prefix" in Tsudick, then the preceding feature of claims 1, 16, and 26 requires that E_{k0} be the "data" or "message" to be transmitted. However, Elgamal does not disclose transmitting E_{k0}. In fact, there is no disclosure in Elgamal, Tsudik, or Ginter of the existence of E_{k0}, namely an encryption of the identification tag (that that identifies the software with the vendor) using the key k(0).

In further response, Applicant asserts that Tsudik's method requires that, in application to the client and server in Elgamal, the client must communicate the secret prefix (i.e., n(0) and

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 160
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

s(*0) in claims 1, 16, 26) to the server in secret (see Tsudik, page 32, lines 10-13). However, claims 1, 16, and 26 recite that the key s(0) is not communicated to the vendor (i.e., the server in Elgamal). Therefore, it is logically impossible to satisfy the requirement of the key s(0) not being communicated to the vendor if Tsudik's "secret prefix" method is used to modify Elgamal.

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

A seventh example of why claims 1, 16, and 26 are not unpatentable over Elgamal in view of Tsudik and further in view of Ginter is that Elgamal in view of Tsudik and further in view of Ginter does not teach or suggest the feature: "said processor, via execution of the feedback module, sending E_{k0}, H_{n0}, and H_{s0} to the database; said processor, via execution of the feedback module, sending E_{k0} and H_{n0} to the vendor".

The Examiner argues: "Ginter further discloses storage of authentication values (Ginter **245:55-62; 246:18-23, 27-50)**... Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik to include ... storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter **222:55-57)**.".

In response, it is not clear that storing E_{k0}, H_{n0},and H_{s0} in the user's database would protect data in the user's database from be accessed by another party as alleged by the Examiner in support of modifying Elgamal in view of Tsudik by storing E_{k0}, H_{n0},and H_{s0} in the user's database.

In further response and assuming that storing E_{k0}, H_{n0},and H_{s0} in the user's database would protect data in the user's database from be accessed by another party (for the sake of

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 161
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

argument only), Applicants assert that the Examiner's reason for modifying Elgamal in view of Tsudik to store E_{k0} and H_{n0} in the user's database ("to be able to securely store data that cannot be accessed by another party in a database at the user's device) is negated by the claimed limitation. "sending E_{k0} and H_{n0} to the vendor" which would enable the vendor to access the very data in the user's device that is intended to be protected from such access by storing E_{k0} and H_{n0} in the user's database in the first place.

Thus, the Examiner's argument is not persuasive.

Therefore, Elgamal in view of Tsudik and further in view of Ginter does not teach the preceding feature of claims 1, 16, and 26.

Based on the preceding arguments, Applicant respectfully maintains that claim 1 is not unpatentable over Elgamal in view of Tsudik and further in view of Ginter, and that claim 1 is in condition for allowance. Since claims 12-15 depend from claim 1, Applicant contends that claims 12-15 are likewise in condition for allowance. Since claims 22-25 depend from claim 16, Applicant contends that claims 22-25 are likewise in condition for allowance. Since claims 32-35 depend from claim 26, Applicant contends that claims 32-35 are likewise in condition for allowance.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 162
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

35 U.S.C. § 103(a): Claims 2-11, 17-21 and 27-31

The Examiner rejected claims 2-11, 17-21 and 27-31 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter "Wheeler").

Since claims 2-11 depend from claim 1, which Applicants have argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter under 35 U.S.C. §103(a), Applicants maintain that claims 2-11 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler under 35 U.S.C. §103(a).

Since claims 17-21 depend from claim 16, which Applicants have argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter under 35 U.S.C. §103(a), Applicants maintain that claims 17-21 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler under 35 U.S.C. §103(a).

Since claims 27-21 depend from claim 26, which Applicants have argued *supra* to not be unpatentable over Elgamal in view of Tsudik and further in view of Ginter under 35 U.S.C. §103(a), Applicants maintain that claims 27-31 are likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler under 35 U.S.C. §103(a).

In addition with respect to claims 2, 17, and 27, Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler does not disclose the feature: "said processor, via

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 163
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

execution of the feedback module, generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and said processor, via execution of the feedback module, sending k(1), n(1), and s(1) to the database"

The Examiner argues:

"Elgamal in view of Tsudik in further view of Ginter does not specifically disclosegenerating a series of keys in which a new key is generated by hashing the last key and using the keys to generate a series of hash values... Wheeler discloses computing a series of keys used to encrypt blocks of data andgenerate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50, 55-59, 66-68)...** Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to include computing a series of keys used ***to encrypt blocks of data*** as disclosed in Wheeler in order to allow the data to be transferred using broadcast transmission (Wheeler Paragraph **53)**" (emphasis added).

In response, Applicants note that the Examiner cites Wheeler for modifying Elgamal "***to encrypt blocks of data***". Yet, the Examiner cites Tsudik "to use the secret prefix method ... ***without using encryption***". Thus, the Examiner's reliance on Wheeler is inconsistent with the Examiner's reliance on Tsudik.

Accordingly, Applicant respectfully contends that the preceding argument by the Examiner is not persuasive.

Therefore, claims 2, 17, and 27 likewise not unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 164
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

CONCLUSION

Based on the preceding arguments, Applicant respectfully believes that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicant invites the Examiner to contact Applicant's representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account 09-0457 (IBM).

Date: 06/30/2009

Jack P. Friedman
Registration No. 44,688

Customer No. 30449
Schmeiser, Olsen & Watts
22 Century Hill Drive - Suite 302
Latham, New York 12110
Telephone (518) 220-1850
Facsimile (518) 220-1857
Email: jfriedman@iplawusa.com

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 165
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

SCORE Placeholder Sheet for IFW Content

Application Number: 11325719 Document Date: 7/1/09

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface using the Supplemental Content tab.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces using the Supplemental Content tab.

Form Revision Date: May 1, 2009

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	Filing Date	☐ To be Mailed
11/325,719	01/05/2006	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		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))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 07/01/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 35	Minus	** 35	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	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	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							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:
/PEGGY YARBOROUGH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. 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	Filing Date	☐ To be Mailed
11/325,719	01/05/2006	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		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))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 07/01/2009

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 35	Minus	** 35	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	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	

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
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:
/PEGGY YARBOROUGH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

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.
11/325,719	01/05/2006	Vijil Enara Chenthamarakshan	IN920050028US1	7235

30449 7590 04/01/2009
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER
NILFOROUSH, MOHAMMAD A

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
04/01/2009	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.	Applicant(s)	
	11/325,719	CHENTHAMARAKSHAN, VIJIL ENARA	
	Examiner	Art Unit	
	MOHAMMAD NILFOROUSH	3685	

-- 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 *05 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* 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 _____ 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)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/5/2006*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 170
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

DETAILED ACTION

Acknowledgements

1. Claims 1-35 are pending.

2. Claims 1-35 have been examined.

3. This Office action is given Paper No. 20090317 for reference purposes only.

Examiner's Comments

4. Applicant's claims employ language that does not serve to differentiate the claims from the prior art.

5. Claim 8 recites "...*if* said executing the iterations has not determined that the first integrity failure has occurred…and *if* n(N+1) = H(N+1) has been determined…" Therefore, the step of "…decrypting E(k(N+1), n(N+1))…" is conditional on not determining that a first integrity failure has occurred and the step of "...ascertaining the integrity of the N feedback entries...." is conditional on determining that n(N+1) = H(N+1) is true. As these steps are not necessarily performed, they do not serve to differentiate the claim from the prior art. Claim 11 recites similar conditional language that does not serve to differentiate the claim from the prior art. Claim 9 further recites "…*if* H'ni = Hni is not determined to be true then ascertaining…" As the step of ascertaining is conditional on H'ni = Hni not being determined to be true, it is not necessarily performed. Accordingly, once the positively recited steps are satisfied, the method as a whole is satisfied -- regardless of whether or not other steps are conditionally performed under certain other hypothetical scenarios. (*In re Johnston*, 77

USPQ2d 1788 (CA FC 2006); *Intel Corp. v. Int'l Trade Comm'n*, 20 USPQ2d 1161 (Fed. Cir. 1991); MPEP §2106 II C).

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

8. Based on Supreme Court precedent (See also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876)) and recent Federal Circuit decisions, a §101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In addition, the tie to a particular apparatus, for example, cannot be mere extra-solution activity. See *In re Bilski*, 88 USPQ2d 1385 (Fed. Cir. 2008).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps.

To meet prong (1), the method step should positively recite the other statutory class (the thing or product) to which it is tied. This may be accomplished by having the claim positively recite the machine that accomplishes the method steps. Alternatively or to meet prong (2), the method step should positively recite identifying the material that is

being changed to a different state or positively recite the subject matter that is being transformed.

In this particular case, claim 1 fails prong (1) because the “tie” (e.g. “…said end user machine comprising the software…”) is representative of extra-solution activity. Claim 26 fails prong (1) because the “tie” (e.g. “…integrating computer-readable code into a computing system…said end user machine comprising the software…”) is representative of extra-solution activity. Additionally, the claim(s) fail prong (2) because the method steps do not transform the underlying subject matter to a different state or thing.

Claims 2-15 are also rejected as each depends from claim 1.

Claims 27-35 are also rejected as each depends from claim 26.

9. Claims 1, 16 and 26 are directed towards a method comprising the steps of "generating a secret key k(0)... generating a secret key n(0)... generating a secret key s(0)... generating an encryption...generating a parameter...generating a parameter...sending...and sending..." However, this claim is directed to an algorithm as these method steps merely manipulate data. MPEP 2106.02 states: if the “acts” of a claimed process manipulate only numbers, abstract concepts or ideas, or signals representing any of the foregoing, the acts are not being applied to appropriate subject matter. *Gottschalk v. Benson*, 409 U.S. 63, 71 - 72, 175 USPQ 673, 676 (1972). Thus, a process consisting solely of mathematical operations, i.e., converting one set of numbers into another set of numbers, does not manipulate appropriate subject matter and thus cannot constitute a statutory process.

Claims 2-15 are also rejected as each depends from claim 1.

Claims 17-25 also rejected as each depends from claim 16.

Claims 27-35 are also rejected as each depends from claim 26.

10. Claims 16-25 are directed to a computer program product. Specifically, Claim 16 recites "A computer program product, comprising a computer usable medium having a computer readable program code embodied therein. However, this is merely software, and it has been held that software without a required computer-readable medium storing software that, *when executed*, causes the computer to perform a particular process or method (MPEP 2106.01) is merely nonfunctional descriptive material and non-statutory under 35 U.S.C. 101.

Claims 17-25 also rejected as each depends from claim 16.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

13. Claims 1, 16, and 26 recite "…making the key n(0) known to the vendor but not to the user…" However, the claims also previously recite "…said end user machine comprising the software, *a feedback module,* and a database…said method comprising, as performed by the *feedback module…*" Thus, the claim recites that the steps of the

method, including the step of "...generating a secret key n(0)…" are performed by a feedback module on the end user machine. It is unclear to one of ordinary skill how the secret key n(0) is not known to the user when it is generated by the end user machine. The claims further recite "...generating a parameter Hn0 such that Hn0 = Hash(n(0) || Ek0)..." It is unclear to one of ordinary skill how the feedback module in the user computer can use n(0) when is only known to the vendor. For purposes of examination, "…generating a secret key n(0) and making the key known to the vendor but not to the user..." is interpreted as generating a key used by the vendor for encryption.

14. Claims 1, 16, and 26 also recite "...making the key...known..." However, it is unclear what action "...making the key...known..." comprises. For purposes of examination, this was interpreted as designated party having some knowledge of the key.

15. Claims 1, 16, and 26 recite the limitation "…an identification tag FE(0)...". However, claims 3, 18, and 28 recite the limitation "…said N feedback entries denoted as FE(1), …, FE(N)…" It is unclear to one of ordinary skill the whether series of data denoted by "FE" consists of identification tags or feedback entries.

16. Claims 2-15, 17-26 and 27-35 are also rejected as each depends on either claim 1, 16, or 26 respectively.

17. An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed (*In re Zletz*, 13 USPQ2d 1320 (Fed. Cir. 1989)).

Claim Rejections - 35 USC § 103

18. 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 negatived by the manner in which the invention was made.

19. Claims 1, 12-16, 22-26, and 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal, et al. (US Patent No. 5,657,390, hereinafter "Elgamal") in view of Tsudik (Reference U) and further in view of Ginter, et al. (US Patent No. 5,892,900, hereinafter “Ginter”)

20. Regarding claims 1, 16, and 26 Elgamal discloses

generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software (Elgamal **2:1-15**; **7:41-51**; **8:5-20**; **33:9-13**);

generating a key by the user terminal that is used for encryption by the vendor (Elgamal **23:9-19**; **28:38-40**; **33:1-4**)

encrypting information to be transferred to the vendor (Elgamal **2:5-10**; **7:2-8**; **8:9-11**; **7:62-8:4**; **13:17-28**; **14:65-68**)

Elgamal further discloses the use of a MAC (message authentication code) to verify the integrity of data that is to be transmitted and that the MAC includes a hash of the data and a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27**).

Elgamal does not specifically disclose generating a key known only to the user, that hash values used to verify the integrity of the data comprise a hash of the data to be transmitted concatenated with the key of the client or server respectively, and that the encrypted data is stored at the client.

Tsudik discloses the use of the secret prefix method of generating a MAC using a hash function. Tsudik discloses that in this method, two principals agree on a secret, S_ab for example, and when A sends a message M to B, it generates an MD4 hash of S_ab concatenated to the beginning of the message such that HashValue = MD4Hash(S_ab || M). The receiver would then use its knowledge of S_ab and the received message to recompute the hash value and compare it to the received hash value to verify the integrity of the message (Tsudik p. **32**, Protocol Description; pp. **33-34** Secret Prefix).

Tsudik in view of Elgamal does not specifically disclose generating a key known only to the user or that the encrypted data is stored at the client.

Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database (Ginter **222:50-61**). Ginter further discloses storage of authentication values (Ginter **245:55-62**; **246:18-23**, **27-50**).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal to use the secret prefix method of generating a message authentication code in order to produce unforgeable integrity values without using encryption so as to provide increased speed by minimizing the use

of encryption software (Tsudik pp. **30-31** Motivation). Further, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik to include the user generating a secure database key known only to the PPE and storing authentication values as disclosed in Ginter in order to be able to securely store data that cannot be accessed by another party in a database at the user's device (Ginter **222:55-57**).

21. Regarding claims 12-13, 21-23, and 32-33, Elgamal discloses that a communication network is disposed between the end user machine and the vendor and permitting the user's machine to access the communication network (Elgamal Abstract **3:24-45**; **4:6-12**; **5:44-50**),

Elgamal does not specifically disclose that an application firewall is disposed between the end user machine and the communication network, that said permitting is controlled by the application firewall, or preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

However, the use of a firewall to permit or prevent a machine to access a network is old and well-known. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to employ a firewall to control access of client machines to a network in order to prevent unauthorized or excessive use of the network.

22. Regarding claims 14, 24, and 34, Elgamal discloses the method of claim 12, wherein the communication network comprises the Internet (Elgamal **3:24-45**; **4:6-12**; **5:44-50**).

23. Regarding claims 15, 25, and 35, Elgamal in view of Tsudik in further view of Ginter does not specifically disclose that the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

However, as the description of the identification tag does not affect the method steps, this is directed towards nonfunctional descriptive material and thus does not serve to differentiate the claims from the prior art. It has been held that where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability …. [T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate (*In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II).

24. Claims 2-11, 17-21, and 27-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Tsudik, in further view of Ginter and further in view of Wheeler (US Patent Application Publication No. 2005/0182932, hereinafter "Wheeler").

25. Regarding claims 2, 3, 17, 18, 27 and 28, Elgamal discloses storing keys in a database at the user terminal (Elgamal **8:33-53**; **16:23-28**), Tsudik discloses the use of the secret prefix method of generating a MAC using a hash function such that

HashValue = MD4Hash(S_ab || M) (Tsudik p. **32**, Protocol Description; pp. **33-34** Secret Prefix), and Ginter discloses discloses storage of authentication values (Ginter **245:55-62**; **246:18-23**, **27-50**).

Elgamal in view of Tsudik in further view of Ginter does not specifically disclose generating a series of keys in which a new key is generated by hashing the last key and using the keys to generate a series of hash values.

Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50**, **55-59**, **66-68**).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Elgamal in view of Tsudik in further view of Ginter to include computing a series of keys used to encrypt blocks of data as disclosed in Wheeler in order to allow the data to be transferred using broadcast transmission (Wheeler Paragraph **53**).

26. Regarding claims 4-6, 19-21, and 29-31,Elgamal discloses generating a key by the user terminal that is used for encryption by the vendor (Elgamal **23:9-19**; **28:38-40**; **33:1-4**) and encrypting information and transferring it to the vendor (Elgamal **2:5-10**; **7:2-8**; **8:9-11**; **7:62-8:4**; **13:17-28**; **14:65-68**). Wheeler further discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each

key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50**, **55-59**, **66-68**).

27. Regarding claims 7 and 10 Elgamal discloses the use of a MAC (message authentication code) to verify the integrity of data and that the MAC includes a hash of the data as well as a secret which can be a client write key, server write key, or a random number (Elgamal **17:50-18:27**). Ginter discloses the use of secure database keys generated in a user's PPE and never exposed to the public in order to encrypt records stored in the PPE's secure database (Ginter **222:50-61**). Ginter further discloses storage of authentication values (Ginter **245:55-62**; **246:18-23**, **27-50**).

28. Regarding claims 8-9 and 11, Wheeler discloses computing a series of keys used to encrypt blocks of data and generate a series of HMAC values, where the recipient both verifies the received keys and the received MAC, and that each key in this series of keys is generated by hashing the key that as generated before it in the series (Wheeler Paragraphs **49-50**, **55-59**, **66-68**). Wheeler discloses verifying whether a received key is valid by comparing the received key to a key independently generated by the recipient by hashing the previously received key (Wheeler Paragraph **57**).

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US Patent Application Publication No. 2002/0112152 to VanHeyningen, et al. for disclosing a client accessing a server through a firewall.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD NILFOROUSH whose telephone number is (571)270-5298. The examiner can normally be reached on Monday-Thursday 8 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on (571)272-6709. 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.

/M. A. N./
Examiner, Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 11/325,719	Applicant(s)/Patent Under Reexamination CHENTHAMARAKSHAN, VIJIL	
	Examiner MOHAMMAD NILFOROUSH	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,657,390 A	08-1997	Elgamal et al.	713/151
*	B	US-5,892,900 A	04-1999	Ginter et al.	726/26
*	C	US-2002/0112152 A1	08-2002	VanHeyningen et al.	713/151
*	D	US-2005/0182932 A1	08-2005	Wheeler, Graham A.	713/168
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Tsudik, Gene. "Message Authentication with One-way Hash Functions." October 1992, ACM SIGCOMM Computer Communication Review. ACM New York, NY, Vol. 22, Issue 5, pp 29-38.
	V	
	W	
	X	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	MOHAMMAD NILFOROUSH	3685

✓	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	03/17/2009								
	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	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	MOHAMMAD NILFOROUSH	3685

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11325719	CHENTHAMARAKSHAN, VIJIL ENARA
	Examiner	**Art Unit**
	Mohammad A Nilforoush	3685

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
Keyword search (see EAST search history)	3/27/2009	/M. A. N./
Search of relevant references (see EAST search history)	3/27/2009	/M. A. N./
Citation search of relevant references (see EAST search history)	3/27/2009	/M. A. N./
Inventor name search (see EAST search history)	3/27/2009	/M. A. N./

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/M. A. N./ Examiner.Art Unit 3685	

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. 7235

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/325,719	01/05/2006 **RULE**	705	3685	IN920050028US1

APPLICANTS
Vijil Enara Chenthamarakshan, Palghat, INDIA;

**** CONTINUING DATA ****************************

**** FOREIGN APPLICATIONS ****************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
02/16/2006

Foreign Priority claimed	❑ Yes ☑ No		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	❑ Yes ☑ No	❑ Met after Allowance	INDIA	12	35	3
Verified and Acknowledged	/MOHAMMAD A NILFOROUSH/ Examiner's Signature	Initials				

ADDRESS

SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110
UNITED STATES

TITLE

System and method for processing feedback entries received from software

FILING FEE RECEIVED		
1750	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

BIB (Rev. 05/07).

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L13	2141	firewall and (hash$3 with key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/27 17:22
L14	800	(verify$3 authenticat$3 comput $3) with (series sequence) with (MAC HMAC (message adj authentication))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/27 17:23
L15	324	L14 and (generat$3 with (sequence series) with key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/27 17:23
L16	28	L15 and firewall	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/27 17:23
L17	1	("5892900").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/27 17:25
L18	1	("5657390").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/27 17:26
S1	49	(US-5790835-$ or US-5664178-$ or US-5963953-$ or US-6092086-$ or US-6119156-$ or US-6175732-$ or US-6212638-$ or US-4819176-$ or US-4924430-$ or US-4968873-$ or US-5243643-$ or US-5414422-$ or US-5432934-$ or US-5506983-$ or US-5581764-$ or US-5627973-$ or US-5630072-$ or US-5695115-$ or US-5696693-$ or US-5706504-$ or US-5715441-$ or US-5774872-$ or US-5913061-$ or US-5948076-$ or US-5999825-$ or US-6038185-$).did. or (US-6085177-$ or US-6097657-$ or US-6141767-$ or US-4447074-$ or US-4579213-$ or US-4817140-$ or US-4912628-$ or US-5186463-$ or US-5225902-$ or US-5235619-$ or US-5251324-$ or US-5255086-$ or US-5291395-$ or US-5379152-$ or US-5420405-$ or US-5428619-$ or US-5610532-$ or US-5666493-$ or US-5680456-$ or US-5737524-$ or US-5737726-$ or US-5758314-$ or US-5758327-$). did.	USPAT	OR	ON	2009/03/16 11:43

S2	50	(US-20070156585-$ or US-20030126400-$ or US-20060126842-$ or US-20080069344-$ or US-20020112166-$ or US-20050081041-$ or US-20060002550-$ or US-20070099597-$ or US-20080075281-$).did. or (US-6640294-$ or US-7035403-$ or US-7359509-$ or US-4490782-$ or US-4881264-$ or US-5202982-$ or US-5297038-$ or US-5347652-$ or US-5375170-$ or US-5392363-$ or US-5432852-$ or US-5440635-$ or US-5440743-$ or US-5450595-$ or US-5475763-$ or US-5483598-$ or US-5502764-$ or US-5521980-$ or US-5579501-$ or US-5600725-$ or US-5608801-$ or US-5613142-$ or US-5623545-$ or US-5625695-$ or US-5633928-$ or US-5655021-$).did. or (US-5664016-$ or US-5692177-$ or US-5696823-$ or US-5713001-$ or US-5719940-$ or US-5719941-$ or US-5742811-$ or US-5752051-$ or US-5754819-$ or US-5790667-$ or US-5796833-$ or US-5799311-$ or US-5805703-$ or US-5825890-$ or US-5835755-$).did.	US-PGPUB; USPAT	OR	ON	2009/03/16 11:43
S8	0	("2007/0156585").URPN.	USPAT	OR	ON	2009/03/16 18:55
S9	7774	feedback with software	US-PGPUB; USPAT	OR	ON	2009/03/16 18:59
S10	1	((verify$3 guarant$4) near2 (authenticity integrity)) with feedback with software	US-PGPUB; USPAT	OR	ON	2009/03/16 19:01
S11	110	(verify$3 autheticat$3) with (database near entry)	US-PGPUB; USPAT	OR	ON	2009/03/17 15:04
S12	1	S11 same (hash$3 with key with (data identifier identification ID))	US-PGPUB; USPAT	OR	ON	2009/03/17 15:05
S13	1	("5265164").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/17 18:56
S14	1	(validat$3 compar$3 check$3) with hash$3 with (key near2 concatenat$3 near3 data)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 19:40
S15	82	(validat$3 compar$3 check$3) with (hash$3 adj3 (key adj3 (data identification id identifier message)))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 19:45
S16	13	S15 and synchroniz$5	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 19:49
S17	6	chentham$.in.	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 20:14

S18	3	synchroniz$5 with (key near version)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 21:52
S19	105	hash$3 with encrypt$3 with ((serial adj number) (license adj key))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 21:54
S20	6	("6047103").PN. OR ("6519701").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 22:13
S21	105	hash$3 with encrypt$3 with ((serial adj number) (license adj key))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 22:33
S22	22	S21 and (concatenat$3)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 22:33
S23	83	S21 not S22	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/17 23:04
S24	1	("6219794").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/23 19:22
S25	148	feedback adj entry	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 14:14
S26	0	feedback adj entry	IBM_TDB	OR	ON	2009/03/24 14:15
S27	3195	feedback	IBM_TDB	OR	ON	2009/03/24 14:15
S29	3	concatenat$3 with key with (value data encrypted)	IBM_TDB	OR	ON	2009/03/24 14:21
S41	7	chenthamarakshan	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 14:45
S42	7	CHENTHAMARAKSHAN	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 14:46
S43	0	CHENTHAMARAKSHAN	IBM_TDB	OR	ON	2009/03/24 14:46
S44	6	CHENTHAMARAKSHAN	FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/24 14:46
S45	3	(autheticating authentication) with communication with vendor with user	FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/03/24 14:48
S46	39	(autheticating authentication) with communication with vendor with user	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 14:49
S47	5	S46 and concatenat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 15:10
S48	7	("20030133464" | "20040034794" | "20040139315" | "20040167859" | "20040210458" | "6842752" | "6901347").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 19:09
S49	0	((verify$3 verification) with checksum) with (sequence near file)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 20:34

S50	0	((verify$3 verification) with checksum) with ((sequence series) near file)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 20:34
S51	2	((verify$3 verification) with checksum) with ((sequence series) near2 file)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 20:34
S52	151	((verify$3 verification) with checksum) with ((sequence series))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 20:44
S53	22	S52 and concatenat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 20:44
S54	370	(concatenat$3 near3 key near4 (data file id identifier tag identification))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 20:47
S55	8	S54 and ((verify$3 verification) with checksum)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 20:47
S56	1	(concatenat$3 near3 key near4 (data file id identifier tag identification)) with checksum	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 21:51
S57	3	(concatenat$3 near3 key near4 (data file id identifier tag identification)) same checksum	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/24 21:52
S58	1	("7414537").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/25 14:08
S59	1	("7415537").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/25 14:09
S60	0	(data adj integrity) with hash$3 with key with concatenat$3	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 15:44
S61	83	(data adj integrity) with hash$3 with key	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 15:44
S62	0	user near2 generat$3 near2 vender near2 key	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 20:07
S63	19050	walker.in.	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 20:07
S64	1322	walker-jay-$.in.	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 20:07
S65	27	S64 and (user with generat$3 with key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 20:07
S66	322	rabin.in.	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 20:16
S67	1	("6006332").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/25 20:18
S68	7	(user near2 generat$3 near2 key) same (user with (transmit$4 near3 key near3 (server vendor host merchant)))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/25 20:19
S69	2	(("7490248") or ("7051204")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/03/25 20:23
S70	249	(vendor host server) with generat $3 with sequence with key	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 14:59

S71	58	S70 and (user with (transmit$4 send$3 transfer$4 forward$3) with key with (vendor server host))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 15:00
S72	52	S71 and (user with generat$3 with key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 15:00
S73	1214	(session adj key) with (vendor host server) with (user client)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 15:46
S74	494	S73 and ((user client) with generat$3 with (session adj key))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 15:46
S75	174	S74 and ((user client) with (transmit$4 transfer$4 send$3 forward$3) with (session adj key) near3 (vendor host server))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 15:47
S76	5	S75 and ((user client) with encrypt$3 near3 (secret adj key) near3 (session adj key))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 15:53
S77	193	S73 and ((user client) near2 generat$3 with (session adj key))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/26 15:57
S78	800	(verify$3 authenticat$3 comput $3) with (series sequence) with (MAC HMAC (message adj authentication))	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/27 14:58
S79	324	S78 and (generat$3 with (sequence series) with key)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/27 14:59
S80	17	S78 and (generat$3 with (sequence series) with key with hash$3)	US-PGPUB; USPAT; USOCR	OR	ON	2009/03/27 14:59

3/27/2009 6:23:14 PM
C:\ Documents and Settings\ mnilforoush\ My Documents\ EAST\ Workspaces\ Mohammad\ 11325719.wsp

Receipt date: 01/05/2006 Express Mail: ET808754613US

INFORMATION DISCLOSURE STATEMENT PURSUANT TO 37 C.F.R. §§1.97-1.99

PATENT APPLICATION

Applicant(s): Vijil Enara Chenthamarakshan Docket No.: IN920050028US1

FOR: **SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE**

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

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56 and pursuant to 37 C.F.R. §§1.97-1.99, Applicant(s) hereby notifies the U.S. Patent and Trademark Office of the documents listed on the attached Form PTO-1449. Applicant respectfully submits that all pending claims are patentable over the foregoing references, alone or in combination. The Examiner is requested to initial the enclosed Form PTO-1449 and return a copy thereof to the undersigned.

The submission of the listed documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant reserves the right to dispute any of the listed documents as prior art during examination. Further, Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application. Furthermore, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made or that no other material information may exist. This Information Disclosure Statement is being filed within three months of the filing date of the captioned patent application, and therefore no certification under 37 C.F.R. §1.97(e) or fee under 37 C.F.R. §1.17(p) is required.

Respectfully submitted,

Dated: 12/01/2005

By Jack P. Friedman
Jack P. Friedman
Reg. No. 44,688

Enclosures: PTO-1449

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.N./

Receipt date: 01/05/2006

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	ATTY DOCKET NO. IN920050028US1	APPLICATION NO.
	APPLICANT(S) Vijil E. Chenthamarakshan	
	FILING DATE	GROUP ART UNIT

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		6,901,347	05/31/2005	Murray, *et al.*			
		6,842,752	01/11/2005	Itabashi, *et al.*			

U.S. PATENT APPLICATION PUBLICATIONS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2004/0210458	10/21/2004	Evans, *et al.*			
		2004/0167859	08/26/2004	Mirabella			
		2004/0139315	07/15/2004	Tokutani, *et al.*			
		2004/0034794	02/19/2004	Mayer, *et al.*			

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

EXAMINER	DATE CONSIDERED
/Mohammad Nilforoush/	03/27/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-A820 (also form PTO-1449) P09C/REV04 Patent and Trademark Office * U.S. DEPARTMENT OF COMMERCE

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.N./

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 194
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Receipt date: 01/05/2006

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

ATTY DOCKET NO.	APPLICATION NO.
IN920050028US1	
Vijil E. Chenthamarakshan	
FILING	GROUP ART

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

U.S. PATENT APPLICATION PUBLICATIONS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2003/0133464	07/17/2003	Marejka, *et al.*			

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

EXAMINER	DATE CONSIDERED
/Mohammad Nilforoush/	03/27/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.N./

Security First Innovations, LLC | Exhibit 2014
Page 2014 - 195
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

PLUS Search Results for S/N 11325719, Searched Mon Mar 16 09:04:08 EDT 2009

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20070156585 68
20030126400 67
20060126842 67
20080069344 67
6640294 66
7035403 66
7359509 66
20020112166 66
20050081041 66
20060002550 66
20070099597 66
20080075281 66
4490782 66
4881264 66
5202982 66
5297038 66
5347652 66
5375170 66
5392363 66
5432852 66
5440635 66
5440743 66
5450595 66
5475763 66
5483598 66
5502764 66
5521980 66
5579501 66
5600725 66
5608801 66
5613142 66
5623545 66
5625695 66
5633928 66
5655021 66
5664016 66
5692177 66
5696823 66
5713001 66
5719940 66
5719941 66
5742811 66
5752051 66
5754819 66
5790667 66
5796833 66
5799311 66
5805703 66
5825890 66
5835755 66

PLUS Search Results for S/N 11325719, Searched Mon Mar 16 09:23:03 EDT 2009

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

5790835 99
5664178 96
5963953 96
6092086 96
6119156 96
6175732 96
6212638 96
6212638 96
4819176 92
4924430 92
4968873 92
5243643 92
5414422 92
5432934 92
5506983 92
5581764 92
5627973 92
5630072 92
5695115 92
5696693 92
5706504 92
5715441 92
5774872 92
5913061 92
5948076 92
5999825 92
6038185 92
6085177 92
6097657 92
6141767 92
4447074 89
4579213 89
4817140 89
4912628 89
5186463 89
5225902 89
5235619 89
5251324 89
5255086 89
5291395 89
5379152 89
5420405 89
5428619 89
5610532 89
5666493 89
5680456 89
5737524 89
5737726 89
5758314 89
5758327 89

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
11/325,719	01/05/2006	Vijil Enara Chenthamarakshan	IN920050028US1

CONFIRMATION NO. 7235

30449
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY12110

Title: System and method for processing feedback entries received from software

Publication No. US-2007-0156585-A1
Publication Date: 07/05/2007

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 703-305-3028.

Pre-Grant Publication Division, 703-605-4283

Express Mail Label No. ET808754613US

22764 U.S. PTO
010506

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

113010 U.S. PTO
11/325719
010506

and invented by:

Vijil Enara Chenthamarakshan
Assignee Name: International Business Machines Corporation
Assignee Address: New Orchard Road
Armonk, NY 10504

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 33 pages and including the following:
   - a. ☒ Descriptive Title of the Invention
   - b. ☐ Cross References to Related Applications *(if applicable)*
   - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   - d. ☐ Reference to Sequence Listing, a Table, or a Computer Program Listing Appendix
   - e. ☒ Background of the Invention
   - f. ☒ Brief Summary of the Invention
   - g. ☒ Brief Description of the Drawings *(if filed)*
   - h. ☒ Detailed Description
   - i. ☒ Claim(s) as Classified Below
   - j. ☒ Abstract of the Disclosure

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 199
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

P01ULRG/REV09

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
   a. ☒ Formal Number of Sheets 12
   b. ☐ Informal Number of Sheets _____
4. ☒ Oath or Declaration
   a. ☒ Newly executed *(original or copy)* ☐ Unexecuted
   b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
   c. ☒ With Power of Attorney ☐ Without Power of Attorney
   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ CD ROM or CD-R in duplicate, large table or Computer Program (Appendix)
7. ☐ Application Data Sheet (See 37 CFR 1.76)
8. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statement(s) Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

9. ☐ Assignment Papers *(cover sheet & document(s))*
10. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
11. ☐ English Translation Document *(if applicable)*
12. ☒ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)* (2)
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☒ Certificate of Mailing
    ☐ First Class ☒ Express Mail *(Specify Label No.)*: ET808754613US

Security First Innovations, LLC, Exhibit 2014
P010LRG/REV09
Page 2014 - 200
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

Accompanying Application Parts (Continued)

17. ☐ Additional Enclosures *(please identify below):*

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

18. ☐ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

19. ☐ Other:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 201
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

Fee Calculation and Transmittal

CLAIMS AS FILED						
For	**#Filed**	**#Allowed**	**#Extra**		**Rate**	**Fee**
Total Claims	35	- 20 =	15	x	$50.00	$750.00
Indep. Claims	3	- 3 =	0	x	$200.00	$0.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
Total # of Pages in Specification		33	**Total # of Drawing Sheets**		12	
Total # of Sheets	45				**Application Size Fee**	$0.00
					Basic Fee	$300.00
					Search Fee	$500.00
					Examination Fee	$200.00
OTHER FEE *(specify purpose)*						$0.00
					TOTAL FILING FEE	$1,750.00

☐ A check in the amount of to cover the filing fee is enclosed.

☒ The Director is hereby authorized to charge and credit Deposit Account No. **09-0457(IBM)** as described below.

- ☒ Charge the amount of **$1,750.00** as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

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

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.

Signature

Dated: 1/3/06

Customer Number: **30449**

cc:

William H. Steinberg
Reg. No. 28,540
IBM Corporation
IP Law Dept.
IQOA/040-3
1701 North St.
Endicott, NY 13760

Security First Innovations, LLC, Exhibit 2014
P01ULRG/REV09
Page 2014 - 202
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10) Applicant(s): **Vijil Enara Chenthamarakshan**			Docket No. **IN920050028US1**	
Application No.	Filing Date	Examiner	Customer No. **30449**	Group Art Unit

Invention: **SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE**

I hereby certify that the following correspondence:

Patent application and corresponding paperwork and IDS

(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

1/05/06
(Date)

Colleen Bulman
(Typed or Printed Name of Person Mailing Correspondence)

Colleen Bulman
(Signature of Person Mailing Correspondence)

ET808754613US
("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

Express Mail ET808754613US

APPLICATION

FOR

UNITED STATES LETTERS PATENT

APPLICANT NAME: Vijil Enara Chenthamarakshan

TITLE: SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

DOCKET NO. IN920050028US1

INTERNATIONAL BUSINESS MACHINES CORPORATION

SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

Background of the Invention

1. Technical Field

The present invention relates to a method and system for processing feedback entries received from software.

2. Related Art

Understanding customer behavior facilitates designing products that are more in tune with customer requirements. As an example, if a vendor finds that a large number of customers are not using the spell checker before sending an email, it may means that the spell check feature should be enabled by default. On the other hand, if a large number of users are dismissing an explicit feature without using the explicit feature, it may mean that the explicit feature is more of an irritant. Currently, most software vendors rely on surveys and interviews to understand customer behavior. However, surveys are often unreliable because survey participants are only a small portion of the installed customer base. Also, survey participants tend to behave differently in survey situations and real life situations.

A situation which may requires immediate attention from software vendors is erroneous program behavior. This includes abnormal terminations, assertion failures, crashes etc. Bugs encountered at customer's site are difficult and expensive to resolve because customers who contact customer support to report such problems often find it difficult to articulate the exact nature of the problem. The customers are also usually not competent to provide accurate information that can help in identifying a problem's cause, such as stack traces, environment etc.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 205
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

It may be desirable for the software to send error reports to the vendor. If the software product sends error reports to the vendor, the error reports could have useful information such as stack traces, crash dumps, etc., which will help the vendor to respond faster to defects, resulting in faster patch release cycles. Some programs provide the user with an option to send error reports to the vendor. If a known problem occurs, the user is provided a link to the service pack, hotfix or knowledge base article that addresses the issue.

Error reports provide the following benefits to software vendors: helps in early identification of critical issues; provides rich information like stack traces, crash dumps, etc., that is assists in reproducing the problem; and provides timely feedback on patches, hotfixes etc., as soon as the problem is detected.

Since user machines are not always online, information collected by the system for error reporting should be stored in user's machine at least until a network connection is available. However, user machines are prone to attacks and the vendor should be able to provide privacy and security for the user even when machines are compromised. However, providing privacy and security even after the user's machine is compromised is a challenging task which is not addressed by existing systems.

Thus, there is a need for an error reporting system that provides security and privacy for the user even after the user's machine is compromised.

Summary of the Invention

The present invention provides a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 206
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, wherein said method comprising, as performed by the feedback module:

generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software;

generating a secret key n(0) and making the key n(0) known to the vendor but not to the user;

generating a secret key s(0) and making the key s(0) known to the user but not to the vendor;

generating an encryption E_{k0} of an identification tag FE(0) such that $E_{k0} = E(k(0),FE(0))$;

generating a parameter H_{n0} such that $H_{n0} = Hash(n(0) \| E_{k0})$;

generating a parameter H_{s0} such that $H_{s0} = Hash(s(0) \| E_{k0})$;

sending E_{k0}, H_{n0}, and H_{s0} to the database; and

sending E_{k0} and H_{n0} to the vendor.

The present invention provides a computer program product, comprising a computer usable medium having a computer readable program code embodied therein, said computer readable program code comprising an algorithm adapted to implement a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, wherein said method

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 207
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

comprising, as performed by the feedback module:

generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software;

generating a secret key n(0) and making the key n(0) known to the vendor but not to the user;

generating a secret key s(0) and making the key s(0) known to the user but not to the vendor;

generating an encryption E_{k0} of an identification tag FE(0) such that $E_{k0} = E(k(0),FE(0))$;

generating a parameter H_{n0} such that $H_{n0} = Hash(n(0) \| E_{k0})$;

generating a parameter H_{s0} such that $H_{s0} = Hash(s(0) \| E_{k0})$;

sending E_{k0}, H_{n0}, and H_{s0} to the database; and

sending E_{k0} and H_{n0} to the vendor.

The present invention provides a process for deploying (or integrating) computing infrastructure, said process comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of performing a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, wherein said method comprising, as performed by the feedback module:

generating a secret key k(0) and making the key k(0) known to both the vendor and a user

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 208
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

of the software;

generating a secret key n(0) and making the key n(0) known to the vendor but not to the user;

generating a secret key s(0) and making the key s(0) known to the user but not to the vendor;

generating an encryption E_{k0} of an identification tag FE(0) such that $E_{k0} = E(k(0),FE(0))$;

generating a parameter H_{n0} such that $H_{n0} = Hash(n(0) \| E_{k0})$;

generating a parameter H_{s0} such that $H_{s0} = Hash(s(0) \| E_{k0})$;

sending E_{k0}, H_{n0}, and H_{s0} to the database; and

sending E_{k0} and H_{n0} to the vendor.

The present invention advantageously provides an error reporting system that provides security and privacy for the user even after the user's machine is compromised.

Brief Description of the Drawings

FIG. 1 depicts a system for processing feedback entries received from software provided by a vendor to an end user machine, in accordance with embodiments of the present invention.

FIG. 2 is a flow chart depicting operation of the system of FIG. 1, in accordance with embodiments of the present invention.

FIG. 3 is a flow chart depicting periodic synchronization of the contents of a database with the vendor of FIG. 1, in accordance with embodiments of the present invention.

FIG. 4 is a flow chart depicting operation of the system of FIG. 1, in accordance with embodiments of the present invention.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 209
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

FIG. 5 is a flow chart depicting generation of secret keys, in accordance with embodiments of the present invention.

FIGS. 6A and 6B is a flow chart depicting setting up the database of FIG. 1, in accordance with embodiments of the present invention.

FIG. 7 is a flow chart depicting storing a feedback entry in the database of FIG. 1, in accordance with embodiments of the present invention.

FIG. 8 is a flow chart depicting synchronizing contents of the database with the vendor of FIG. 1, in accordance with embodiments of the present invention.

FIG. 9 is a flow chart describing verification, by the vendor of FIG. 1, of the integrity of the feedback entries received by the vendor, in accordance with embodiments of the present invention.

FIG. 10 is a flow chart describing verification, by the user of FIG. 1, of the integrity of the feedback entries in the database, in accordance with embodiments of the present invention.

FIG. 11 illustrates a computer system used for processing feedback entries received from software provided by a vendor to an end user machine, in accordance with embodiments of the present invention.

Detailed Description of the Invention

The present invention provides a secure way of collecting program usage statistics that also protects the privacy of individual users, by using an application firewall, a separate feedback module, a secure database and a special purpose cryptographic protocol. Apart from protecting users from malicious attackers, the present invention also prevents the software vendor from misleading the user on what information was sent to its site for analysis. In other words, the

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 210
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

present invention treats even the software vendor as a potential adversary. Also, the present invention invention describes a mechanism that provides security and privacy even when the user's system is taken over by an adversary.

By using this present invention, users will have exact control over the data that is sent to the vendor and will facilitate a huge increase in adoption of automated feedback and error reporting. In fact, when users become more and more aware of online privacy issues, they will insist that all automated feedback and error reporting systems should include mechanisms that provide security and privacy.

The present invention provides an automated feedback and error reporting system that is not too invasive, so that software vendors may employ prudence while deciding what information is collected. In addition, the present invention enables the user to have a fool proof way to ensure that the privacy policy agreed upon by the vendor is kept, so that if there is a breach of privacy, the user would be able to detect the breach.

The present invention enables users to periodically check for privacy policy violations, so that the user may read at any time the information that was sent to the vendor, and nobody other than the vendor and the user are able to read the information that was sent by the software. The vendor is able to verify that all information that was received was actually sent by the software and was not modified in transit. The system is able to function (with all the privacy and security guarantees) even when there is no network connection available to communicate with the vendor.

User machines are prone to attacks and the feedback module of the present invention is able to provide privacy and security even when user machines are compromised. As a first example, if the vendor attacks the user machine and the user's machine is compromised as a

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 211
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

result, the vendor should not be able to modify or delete information that was collected (and kept in user's machine) before the compromise and escape detection by the user. As a second example, if the user machine is compromised, any attacker (other than the vendor) should not be able to read the information collected from the user before the compromise. As a third example, if the user machine is compromised, the attacker should not be able to modify or delete information collected from the user before the compromise and escape detection by the vendor or user.

A concatenation operator || is defined such that A || B denotes a concatenation of character strings A and B. For example if A = "abc" and B = "xyz" then A || B = "abcxyz".

E(K,X) is defined as a symmetric key encryption of a parameter X using a key K. E(K,X) results from use of an encryption algorithm such as Data Encryption Standard (DES) or Advanced Encryption Standard (AES), wherein the data cannot be decrypted without the knowledge of the key k.

Hash(Y) is defined as a one way hash function of a parameter Y using a hash algorithm such as MD5 (RFC1321) or SHA1 (RFC3174). Hash(Y) has the following properties: given the Hash(M), it is difficult to find the message M. Hash(Y) is preimage resistant: given a message M1, it is difficult to find another message M2 such that Hash(M1) = Hash(M2). Hash(Y) is collision resistant: it is difficult to find two messages M1 and M2 such that Hash(M1) = Hash(M2).

FIG. 1 depicts a system10 for processing feedback entries received from software 13 provided by a vendor 18 to an end user machine 12, in accordance with embodiments of the present invention. The vendor 18 comprises the vendor's computing site which includes, *inter alia*, a server of the vendor 18. The end user machine 12, which comprises a computer or

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 212
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

computer system, includes a feedback module (FBM) 14, a database 15, and the software 13. The database 15 is a secure database due to security features of the present invention as described *infra*. The feedback module 14 is connected to the vendor 18 via a communication network 17 (e.g., the Internet). The communication network 17 is disposed between the end user machine 12 and the vendor 18. A user 19, who uses the software 13 provided by the vendor 18, may be online with respect to the end user machine 12.

Access by feedback module 14 to the communication network 17 is controlled by an application firewall 16 which is disposed between the end user machine 12 and the communication network 17. The application firewall 16 is adapted to permit access by the feedback module 14 to the communication network 17. The application firewall 16 is adapted to prevent access by the software to the communication network 17. Accessing the communication network 17 comprises sending data to the communication network 17 and/or receiving data from the communication network 17. The application firewall 16 consults its internal rule database before allowing any application to access the communication network 17. Examples of application firewalls include Zone Labs Integrity Desktop.

The system 10 comprises the feedback module 14 and the database 15.

The software 13, which is installed by the vendor 18 in the end user machine 12, is prevented from directly accessing the vendor 18 by the application firewall 16. Instead, the feedback module 14 communicates with the vendor 18. When the software13 has information to send to the vendor 18, the software13 sends the information to the feedback module 14 as feedback entries. It is assumed herein that the vendor has knowledge of the format used to encode the feedback entries. The feedback module 14 provides security and privacy for the user 19. The feedback module 14 writes the feedback entries to the database 15 after following a

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 213
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

protocol described *infra*. Then, if a network connection from the feedback module 14 to the vendor 18 is available, the feedback module 14 follows a synchronization protocol (see FIG. 8) to sync the contents of the database 15 with the vendor 18. The application firewall 16 is configured to allow the feedback module 14 to connect to the vendor 18 and to prevent all other programs from accessing the vendor 18. If the synchronization is successful, the vendor 18 can verify the integrity of data received by the vendor 18 by following the algorithm given in FIG. 9. The user can verify whether or not all the security requirements are met by following the algorithm given in FIG. 10.

FIG. 2 is a flow chart depicting the operation of the system 10 of FIG. 1, in accordance with embodiments of the present invention. The flow chart of FIG. 2 comprises steps 21-25. Step 21 provides initializations, including setup of secret keys and setup of the database 15 to be secure for the feedback module 14 and the vendor 18. Step 22 executes the software 13. The feedback module 14 executes a loop comprising steps 23-25, wherein each pass through the loop performs operations on feedback entries generated by the software 13. In step 23, the software 13 generates feedback entries which are processed by the feedback module 14 in step 24. In step 25, the feedback module 14 writes the processed feedback entries to the database 15.

FIG. 3 is a flow chart depicting periodic synchronization of the contents of the database 15 with the vendor 18 of FIG. 1, in accordance with embodiments of the present invention. The synchronization is performed by the feedback module 14 periodically in accordance with a specified synch interval of time. The sync interval may be specified by vendor 18 or chosen by the user 19. The flow chart of FIG. 3 comprises steps 31-35. The process loops through step 31 until it is determined that the current synch interval has expired so that a synchronization may next be performed. Step 32 determines whether a synchronization is required. For example, a

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 214
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

synchronization is required if the feedback module 14 has received a feedback entry from the software 13 since the last synchronization. If a synchronization is not required, then the process returns to step 31. If a synchronization is required, then step 33 is performed. The process loops through step 33 until it is determined that the user 19 is online with respect to the end user machine 12, which triggeres execution of step 34. In step 34, the feedback module 14 synchronizes the contents of the database 15 with the vendor 18, as described *infra* in conjunction with FIG. 8. In step 35, the vendor 18 checks the integrity of the data received by the vendor 18, as described *infra* in conjunction with FIG. 9.

The feedback module 14 receives messages (feedback entries which could include usage statistics, error reports etc.) from the software 13 and writes the messages to the database 15 (which is secure) to assure security and privacy. The cryptographic protocols that support the security and privacy involve various interactions between the various entities. The entities are: the vendor 18 who can be contacted through the public Internet but access to whom is denied to all software programs except the feedback module 14 by the application firewall 16; the user 19 of the software 13 provided by the vendor 18; and the feedback module 14 which is a software program which interacts with the software 13 provided by the vendor 18.

FIG. 4 is a flow chart depicting operation of the system 10 of FIG. 1, in accordance with embodiments of the present invention. The flow chart of FIG. 4, which is more detailed than the flow chart of FIG. 2, comprises steps 41-46.

Step 41 of FIG. 4 generates secret keys between the vendor 18 and the feedback module 14. In step 41, the feedback module 14 establishes two secret keys, namely k(0) and n(0), that are shared between the feedback module 14 and the vendor 18. Generation of keys k(0) and n(0) can be done using a public key algorithm such as, *inter alia*, Diffie-Hellman key exchange.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 215
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Alternatively, if the public key of the vendor 18 is available to the feedback module 14 as a public key certificate, then the keys k(0) and n(0) can be negotiated using a protocol such as Secure Sockets Layer (SSL). The feedback module 14 makes the secret key k(0) available to both the vendor 18 and the user 19. In general, any method known to a person of ordinary skill in the art for establishing two secret keys is within the scope of the present invention.

The feedback module 14 also generates an identification tag, denoted illustratively as FBM_ID, that helps in uniquely identifying this installation of the software 13 with the vendor 18. This identification tag could be the serial number of the software, version number for the software, a combination of the serial number of the software and the version number of the software, etc. The feedback module 14 discloses this identification tag to the user 19.

The same feedback module 14 could support multiple vendors (e.g., two or more vendors) such that two secret keys are generated for each vendor of the multiple vendors.

In step 42 of FIG. 4, the feedback module 14 generates a secret key s(0) for use between the user 19 and the feedback module 14. The feedback module 14 discloses the secret key s(0) to the user 19. The secret key s(0) can be derived, *inter alia*, from a password that is known only to the user 19, by hashing the password using a one way hash function.

FIG. 5 is a flow charting depicting steps 41 and 42 of FIG. 4, wherein steps 41-42 generate the secret keys k(0) and n(0) (step 41) and s(0) (step 42). The flow chart of FIG. 5 comprises steps 51-55. Step 51 generates the secret keys k(0) and n(0). Step 52 sends the generated secret keys k(0) and n(0) to the vendor 18 securely. Step 53 prompts the user 19 for a password "P". Step 54 generates the secret key s(0) as a hash of the password P (i.e., as Hash(P)). Step 55 sends k(0) and n(0) to the vendor 18 securely. Although FIG. 5 depicts step 55 after steps 53 and 54, step 55 may be performed either before or after steps 53 and 54.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 216
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Note that after steps 41 and 42 of FIG. 4 are performed, the secret keys k(0), n(0), and s(0) are known as follows. The key k(0) is known to the feedback module 14, the vendor 18, and the user 19. The key n(0) is known to the feedback module 14 and the vendor 18. The key s(0) is known to the feedback module 14 and the user 19. The keys k(0), n(0), and s(0), as well as all other keys described herein, may be in a character string format.

Step 43 of FIG. 4 sets up the database 15, which is described in a flow chart in FIGS. 6A and 6B (collectively, "FIG. 6"), in accordance with embodiments of the present invention. The flow chart of FIG. 6 comprises steps 60-69. The feedback module 14 performs steps 60-64 (FIG. 6A), and the vendor 18 performs steps 65-69 (FIG. 6B).

In step 60, the feedback module 14 sets parameter FE(0) equal to the identification tag denoted illustratively as FBM_ID. In step 61, the feedback module 14 calculates parameters E_{k0}, H_{n0}, and H_{s0}:

$E_{k0} = E(k(0), FE(0))$

$H_{n0} = Hash(n(0) \| E_{k0})$

$H_{s0} = Hash(s(0) \| E_{k0})$

In step 62, feedback module 14 generates keys k(1), n(1), and s(1):

$k(1) = Hash(k(0))$

$n(1) = Hash(n(0))$

$s(1) = Hash(s(0))$

In step 63, the feedback module 14 writes E_{k0}, H_{n0}, H_{s0}, k(1), n(1), and s(1) to the database 15.

In step 64, the feedback module 14 sends E_{k0} and H_{n0} to the vendor 18.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 217
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In step 65, the vendor 18 calculates $H'_{n0} = Hash(n(0) \| E_{k0})$ from E_{k0} received by the vendor 18, using the key n(0) in the possession of the vendor 18. Step 66 determines whether the vendor-calculated H'_{n0} matches the H_{n0} received by the vendor 18 from the feedback module 14 as a result of step 64. If step 66 determines that H'_{n0} does not match H_{n0}, then an error or a breach of security has occurred and the process stops in step 67. If step 66 determines that H'_{n0} matches H_{n0}, then step 68 is executed in which the vendor 18 decrypts E_{k0} using the key k(0) from which FE(0) is determined. In step 69, the vendor 18 records that the database 15 is set. Since n(0) is known only to the vendor 18 and the feedback module 14, the vendor 18 has determined that E_{k0} was properly received from the feedback module 14 via step 64.

In step 44 of FIG. 4, the feedback module 14 stores a feedback entry in the database 15, which is described in detail in a flow chart in FIG. 7, in accordance with embodiments of the present invention. The flow chart of FIG. 7 comprises steps 71-75, which are performed by the feedback module 14. In step 71, the feedback module 14 receives a new feedback entry FE(i) from the software 13, wherein i =1 for the first such new feedback entry FE(i). In step 72, the feedback module 14 calculates parameters E_{ki}, H_{ni}, and H_{si}:

$$E_{ki} = E(k(i), FE(i))$$

$$H_{ni} = Hash(n(i) \| E_{ki})$$

$$H_{si} = Hash(s(i) \| E_{ki})$$

In step 73, the feedback module 14 writes E_{ki} , H_{ni}, and H_{si} to the database 15. In step 74, the feedback module 14 generates new keys k(i+1), n(i+1), and s(i+1):

$$k(i+1) = Hash(k(i))$$

$$n(i+1) = Hash(n(i))$$

$$s(i+1) = Hash(s(i))$$

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 218
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In step 75, the feedback module 14 replaces k(i), n(i), and s(i) with keys k(i+1), n(i+1), s(i+1), respectively, in the database 15. For example, the feedback module 14 may erase keys k(i), n(i), and s(i) from the database 15 and write keys k(i+1), n(i+1), s(i+1) to the database 15.

Steps 71-75 are executed for each new feedback entry received by the feedback module 14 from the software 13. If N such new feedback entries are processed by the feedback module 14, then after the N new feedback entries have been processed in accordance with steps 71-75, the database 15 will comprise E_{ki}, H_{ni}, and H_{si} and for i = 1, 2, ..., N, and the database 15 will additionally comprise k(N+1), n(N+1), and s(N+1).

In step 45 of FIG. 4, the feedback module 14 synchronizes contents of the database 15 with the vendor 18, which is described in detail in a flow chart in FIG. 8, in accordance with embodiments of the present invention. The flow chart of FIG. 8 comprises steps 81-85, which are performed periodically by the feedback module 14.

Step 81 sets an index i equal to 0. Steps 82-84 define a loop in which the index i is executed from i = 0 to i = N, wherein N is the number of feedback entries in the database 15. The index i is a feedback entry index for i = 1, 2, ..., N. Step 82 tests for the end of the loop (i.e., for i > N). If step 82 determines that i is not greater than N, then step 83 is next executed and sends E_{ki} and H_{ni} to the vendor 15, followed by incrementing i by 1 in step 84 to complete the ith iteration of the loop. If step 82 determines that i > N, then step 85 is next executed to send an encryption of n(N+1), using the key k(N+1), to the vendor 18 which ends the synchronization process, said encryption sent to the vender 18 being expressed as E(k(N+1), n(N+1)).

Alternatively, instead of sending all the feedback entries in the database 15 to the vendor 18, the synchronization protocol can send only those feedback entries that were added since the last synchronization.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 219
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

In step 45 of FIG. 4, the integrity of the feedback entries are verified by the vendor 18 (see FIG. 9) and by the user (see FIG. 10).

FIG. 9 is a flow chart describing verification of the integrity of the feedback entries received by the vendor 18, in accordance with embodiments of the present invention. The flow chart of FIG. 9 comprises steps 111-120, which are performed by the vendor 18. The inputs to the process of FIG. 9 are the following parameters previously received by the vendor 18:

(1) keys n(0) and k(0) from step 41 of FIG. 4;

(2) E_{k0} and H_{n0} from step 64 of FIG. 6A;

(3) N = number of feedback entries received by vendor 18

(4) E_{ki} and H_{ni} (i=1, 2, ..., N) from step 83 of FIG. 8; and

(5) E(k(N+1),n(N+1)) from step 85 of FIG. 8.

Step 111 initializes an iteration index i to 0 and calculates H(0):

$$H(0) = n(0) \text{ (using the input key } n(0))$$

Next, a loop comprising steps 112-117 is executed.

Step 112 calculates H'_{ni}:

$$H'_{ni} = \text{Hash}(H(i) \,||\, E_{ki})$$

using the input E_{k0} if i=0 or the input E_{ki} if i > 1, and using H(0) from step 111 if i=0 or H(i) from step 115 of previous iteration of the loop if i > 0.

Step 113 determines whether H'_{ni} is equal to H_{ni}, using the input H_{n0} if i=0 or the input H_{ni} if i > 1. If step 113 determines that H'_{ni} is unequal to H_{ni} then step 114 is executed wherein step 114 announces that an integrity failure has occurred. If step 113 determines that $H'_{ni} = H_{ni}$ then step 115 is next executed.

Step 115 calculates:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 220
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

$H(i+1) = Hash(H(i))$ and

$k(i+1) = Hash(k(i))$

The computation of $k(i+1)$ uses the input key $k(0)$ if $i = 0$ or uses $k(i)$ from step 115 of the previous iteration of the loop if $i > 0$.

Step 116 ascertains whether to exit the loop by determining whether $i > N$. If step 116 determines that i does not exceed N, then step 117 is executed to increment i by 1, followed by looping back to step 112 to perform the next iteration of the loop. If step 116 determines that $i > N$, then the loop is exited and step 118 is next performed.

Step 118 decrypts $E(k(N+1), n(N+1))$ (input from step 85 of FIG. 8), using the key $k(N+1)$ from step 115 of the last iteration of the loop, to infer $n(N+1)$.

Step 119 determines whether the inferred $n(N+1)$ equals $H(N+1)$, wherein $H(N+1)$ was calculated in step 115 of the last iteration of the loop. If step 119 determines that $n(N+1)$ does not equal $H(N+1)$ then step 120 is executed wherein step 120 announces that an integrity failure has occurred. If step 119 determines that $n(N+1) = H(N+1)$ then the verification by the vendor 18 ends.

FIG. 10 is a flow chart describing verification of the integrity of the feedback entries in the database 15, in accordance with embodiments of the present invention. The flow chart of FIG. 10 comprises steps 131-139, which are performed by the user 19. The inputs to the process of FIG. 9 are the following parameters previously inserted into the database 15 by the feedback module 14:

(1) key $s(0)$ from step 42 of FIG. 4;

(2) E_{k0} and H_{s0} from step 63 of FIG. 6A;

(3) N = number of feedback entries in database 15

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 221
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

(4) E_{ki} and H_{si} (i=1, 2, …, N) from step 73 of FIG. 7;

(5) s(N+1) from step 75 of FIG. 7

Step 131 initializes an iteration index i to 0 and calculates S(0):

$$S(0) = s(0) \text{ (using the input key } s(0))$$

Next, a loop comprising steps 132-137 is executed.

Step 132 calculates H'_{si}:

$$H'_{si} = \text{Hash}(S(i) \,||\, E_{ki})$$

using the input E_{k0} if i=0 or the input E_{ki} if i > 1, and using S(0) from step 131 if i=0 or S(i) from step 135 of the previous iteration of the loop if i > 0.

Step 133 determines whether H'_{si} is equal to H_{si}, using the input H_{s0} if i=0 or the input H_{si} if i > 1. If step 133 determines that H'_{si} is unequal to H_{si} then step 134 is executed wherein step 134 announces that an integrity failure has occurred. If step 133 determines that $H'_{si} = H_{si}$ then step 135 is next executed.

Step 135 calculates:

$$S(i+1) = \text{Hash}(S(i))$$

Step 136 ascertains whether to exit the loop by determining whether i > N. If step 136 determines that i does not exceed N, then step 137 is executed to increment i by 1, followed by looping back to step 132 to perform the next iteration of the loop. If step 136 determines that i > N, then the loop is exited and step 138 is next performed.

Step 138 determines whether S(N+1) equals s(N+1), wherein S(N+1) was calculated in step 135 of the last iteration of the loop, and wherein s(N+1) is obtained from the database 15. If step 138 determines that S(N+1) does not equal s(N+1) then step 139 is executed wherein step

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 222
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

139 announces that an integrity failure has occurred. If step 138 determines that S(N+1) = s(N+1) then the verification by the user 19 ends.

For the purpose of security, the application firewall 16 prevents all communication between the software 13 and the vendor 18 and ensures that only the feedback module 14 is allowed to communicate with the vendor 18. Hence, the software 13 cannot send arbitrary entries without the arbitrary entries getting recorded by the feedback module 14. The feedback module 14 maintains all of the feedback entries sent to the vendor18 in the database 15 so that the feedback entries can be verified by the user19 at any time. Different keys are used for encrypting and verifying each feedback entry. Each key is derived from the previous key, but given a key, its previous version cannot be found since a one way hash function is used to derive newer keys. At the time of intrusion, the intruder has access only to the latest values of the keys k(i+1), n(i+1) and s(i+1). All communication between the feedback module 14 and vendor 18 is encrypted using k(i) which is not known to others. Since there is no way for the intruder to derive previous values of the keys, the intruder cannot forge or read or delete previous feedback entries that were created prior to the intrusion. Note that two verification keys (n(0) and s(0)) are used, one verification key for the vendor 18 and the other verification key for the user 19, which ensures that if the vendor 18 becomes the intruder, the user 19 can still locate any forgery.

FIG. 11 illustrates a computer system 90 used for processing feedback entries received from software provided by a vendor to an end user machine, in accordance with embodiments of the present invention. Either or both of the end user machine 12 and the computer system of the vendor 18 of FIG. 1 may comprise the computer system 90 of FIG. 11.

The computer system 90 comprises a processor 91, an input device 92 coupled to the processor 91, an output device 93 coupled to the processor 91, and memory devices 94 and 95

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 223
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

each coupled to the processor 91. The input device 92 may be, *inter alia*, a keyboard, a mouse, etc. The output device 93 may be, *inter alia*, a printer, a plotter, a computer screen, a magnetic tape, a removable hard disk, a floppy disk, etc. The memory devices 94 and 95 may be, *inter alia*, a hard disk, a floppy disk, a magnetic tape, an optical storage such as a compact disc (CD) or a digital video disc (DVD), a dynamic random access memory (DRAM), a read-only memory (ROM), etc. The memory device 95 includes a computer code 97.

The computer code 97 includes an algorithm for processing feedback entries received from software provided by a vendor to an end user machine. The computer code 97 may represent the feedback module 14 of FIG. 1 if the end user machine 12 comprises the computer system 90. The computer code 97 may represent software of the vendor 18 if the computer system of the vendor 18 comprises the computer system 90.

The processor 91 executes the computer code 97. The memory device 94 includes input data 96. The input data 96 includes input required by the computer code 97. The output device 93 displays output from the computer code 97. Either or both memory devices 94 and 95 (or one or more additional memory devices not shown in FIG. 11) may be used as a computer usable medium (or a computer readable medium or a program storage device) having a computer readable program code embodied therein and/or having other data stored therein, wherein the computer readable program code comprises the computer code 97. Generally, a computer program product (or, alternatively, an article of manufacture) of the computer system 90 may comprise said computer usable medium (or said program storage device).

Thus the present invention discloses a process for deploying or integrating computing infrastructure, comprising integrating computer-readable code into the computer system 90, wherein the code in combination with the computer system 90 is capable of performing a method

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 224
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

for processing feedback entries received from software provided by a vendor to an end user machine.

While FIG. 11 shows the computer system 90 as a particular configuration of hardware and software, any configuration of hardware and software, as would be known to a person of ordinary skill in the art, may be utilized for the purposes stated *supra* in conjunction with the particular computer system 90 of FIG. 11. For example, the memory devices 94 and 95 may be portions of a single memory device rather than separate memory devices.

While embodiments of the present invention have been described herein for purposes of illustration, many modifications and changes will become apparent to those skilled in the art. Accordingly, the appended claims are intended to encompass all such modifications and changes as fall within the true spirit and scope of this invention.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 225
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

CLAIMS

What is claimed is:

1. A method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, wherein said method comprising, as performed by the feedback module:

generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software;

generating a secret key n(0) and making the key n(0) known to the vendor but not to the user;

generating a secret key s(0) and making the key s(0) known to the user but not to the vendor;

generating an encryption E_{k0} of an identification tag FE(0) such that $E_{k0} = E(k(0),FE(0))$;

generating a parameter H_{n0} such that $H_{n0} = Hash(n(0) \| E_{k0})$;

generating a parameter H_{s0} such that $H_{s0} = Hash(s(0) \| E_{k0})$;

sending E_{k0}, H_{n0}, and H_{s0} to the database; and

sending E_{k0} and H_{n0} to the vendor.

2. The method of claim 1, said method comprising, as performed by the feedback module:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 226
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

sending k(1), n(1), and s(1) to the database.

3. The method of claim 2, said method comprising, as performed by the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), ..., FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, ..., N comprising:

calculating parameters E_{ki}, H_{ni}, and H_{si} such that E_{ki} = E(k(i), FE(i)), H_{ni} = Hash(n(i) || E_{ki}), and H_{si} = Hash(s(i) || E_{ki});

writing E_{ki}, H_{ni}, and H_{si} to the database;

generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

4. The method of claim 3, said method comprising, as performed by the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, ..., N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

5. The method of claim 4, wherein M=1.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 227
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

6. The method of claim 4, wherein M>1.

7. A validation method for validating the N feedback entries resulting from performance of the method of claim 4, said validation method comprising verifying, by the vendor, an integrity of the N feedback entries received by the vendor as a result of said sending to the vendor: $((E_{ki}, H_{ni}), i = M, \ldots, N)$ and $E(k(N+1), n(N+1))$, wherein $1 \leq M \leq N$.

8. The validation method of claim 7, wherein said verifying comprises:

setting $i = 0$ and $H(0) = n(0)$;

executing iterations $i = 0, 1, \ldots, N$ of a loop, wherein executing each iteration i of the loop comprises: setting $H'_{ni} = Hash(H(i) \| E_{ki})$; determining if $H'_{ni} = H_{ni}$ is true; and if $H'_{ni} = H_{ni}$ is determined to be true then setting $H(i+1) = Hash(H(i))$ and $k(i+1) = Hash(k(i))$, otherwise ascertaining that a first integrity failure has occurred;

if said executing the iterations has not determined that the first integrity failure has occurred then after said executing:

decrypting $E(k(N+1), n(N+1))$ using key $k(N+1)$ to infer $n(N+1)$;

determining if $n(N+1) = H(N+1)$ is true; and

if $n(N+1) = H(N+1)$ has been determined to be true then ascertaining that the integrity of the N feedback entries received by the vendor has been verified, otherwise ascertaining that a second integrity failure has occurred.

9. The validation method of claim 7, wherein the validation method further comprises, as performed by the vendor prior to said verifying:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 228
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

calculating $H'_{n0} = Hash(n(0) \| E_{k0})$;

determining if $H'_{n0} = H_{n0}$ is true; and

if $H'_{ni} = H_{ni}$ is not determined to be true then ascertaining that an error has occurred, otherwise decrypting E_{ko} to infer FE(0) and recording that the database is set.

10. A validation method for validating the N feedback entries resulting from performance of the method of claim 3, said validation method comprising verifying, by the user, an integrity of the N feedback entries in the database as a result of writing $((E_{ki}, H_{ni}, H_{si}), i= 1, \ldots, N)$ to the database.

11. The validation method of claim 10, wherein said verifying comprises:

setting $i = 0$ and $S(0) = s(0)$;

executing iterations $i = 0, 1, \ldots, N$ of a loop, wherein executing each iteration i of the loop comprises: setting $H'_{si} = Hash(S(i) \| E_{ki})$; determining if $H'_{si} = H_{si}$ is true; and if $H'_{si} = H_{si}$ is determined to be true then setting $S(i+1) = Hash(S(i))$, otherwise ascertaining that a first integrity failure has occurred;

if said executing the iterations has not determined that the first integrity failure has occurred then after said executing:

determining if $S(N+1) = s(N+1)$; and

if $S(N+1) = s(N+1)$ has been determined to be true then ascertaining that the integrity of the N feedback entries in the database has been verified, otherwise ascertaining that a second integrity failure has occurred.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 229
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

12. The method of claim 1, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, and wherein the method further comprises permitting the feedback module to access the communication network, said permitting being controlled by the application firewall.

13. The method of claim 12, wherein the method further comprises preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

14. The method of claim 12, wherein the communication network comprises the Internet.

15. The method of claim 1, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 230
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

16. A computer program product, comprising a computer usable medium having a computer readable program code embodied therein, said computer readable program code comprising an algorithm adapted to implement a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, wherein said method comprising, as performed by the feedback module:

generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software;

generating a secret key n(0) and making the key n(0) known to the vendor but not to the user;

generating a secret key s(0) and making the key s(0) known to the user but not to the vendor;

generating an encryption E_{k0} of an identification tag FE(0) such that $E_{k0} = E(k(0),FE(0))$;

generating a parameter H_{n0} such that $H_{n0} = Hash(n(0) \| E_{k0})$;

generating a parameter H_{s0} such that $H_{s0} = Hash(s(0) \| E_{k0})$;

sending E_{k0}, H_{n0}, and H_{s0} to the database; and

sending E_{k0} and H_{n0} to the vendor.

17. The computer program product of claim 16, said method comprising, as performed by the feedback module:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 231
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

sending k(1), n(1), and s(1) to the database.

18. The computer program product of claim 17, said method comprising, as performed by the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), ..., FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, ..., N comprising:

calculating parameters E_{ki}, H_{ni}, and H_{si} such that E_{ki} = E(k(i), FE(i)), H_{ni} = Hash(n(i) || E_{ki}), and H_{si} = Hash(s(i) || E_{ki});

writing E_{ki}, H_{ni}, and H_{si} to the database;

generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

19. The computer program product of claim 18, said method comprising, as performed by the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, ..., N) and E(k(N+1), n(N+1)), wherein $1 \leq M \leq N$.

20. The computer program product of claim 19, wherein M=1.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 232
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

21. The computer program product of claim 19, wherein M>1.

22. The computer program product of claim 16, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, and wherein the method further comprises permitting the feedback module to access the communication network, said permitting being controlled by the application firewall.

23. The computer program product of claim 22, wherein the method further comprises preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

24. The computer program product of claim 22, wherein the communication network comprises the Internet.

25. The computer program product of claim 16, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 233
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

26. A process for deploying (or integrating) computing infrastructure, said process comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of performing a method for processing feedback entries received from software, said software provided by a vendor to an end user machine, said end user machine comprising the software, a feedback module, and a database, wherein a concatenation operator || is defined such that A || B denotes a concatenation of strings A and B, wherein E(K,X) defines a symmetric key encryption of a parameter X using a key K, wherein Hash(Y) defines a one way hash function of a parameter Y, wherein said method comprising, as performed by the feedback module:

generating a secret key k(0) and making the key k(0) known to both the vendor and a user of the software;

generating a secret key n(0) and making the key n(0) known to the vendor but not to the user;

generating a secret key s(0) and making the key s(0) known to the user but not to the vendor;

generating an encryption E_{k0} of an identification tag FE(0) such that $E_{k0} = E(k(0),FE(0))$;

generating a parameter H_{n0} such that $H_{n0} = Hash(n(0) \| E_{k0})$;

generating a parameter H_{s0} such that $H_{s0} = Hash(s(0) \| E_{k0})$;

sending E_{k0}, H_{n0}, and H_{s0} to the database; and

sending E_{k0} and H_{n0} to the vendor.

27. The process of claim 26, said method comprising, as performed by the feedback module:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 234
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

generating keys k(1), n(1), and s(1) such that k(1) = Hash(k(0)), n(1) = Hash(n(0)), and s(1) = Hash(s(0)); and

sending k(1), n(1), and s(1) to the database.

28. The process of claim 27, said method comprising, as performed by the feedback module, receiving N feedback entries from the software and processing the N feedback entries, said N feedback entries denoted as FE(1), …, FE(N), said N at least 1, said processing the feedback entry FE(i) for each of i = 1, …, N comprising:

calculating parameters E_{ki}, H_{ni}, and H_{si} such that E_{ki} = E(k(i), FE(i)), H_{ni} = Hash(n(i) || E_{ki}), and H_{si} = Hash(s(i) || E_{ki});

writing E_{ki}, H_{ni}, and H_{si} to the database;

generating keys k(i+1), n(i+1), and s(i+1) such that k(i+1) = Hash(k(i)), n(i+1) = Hash(n(i)), and s(i+1) = Hash(s(i)); and

replacing keys k(i), n(i), and s(i) in the database with keys k(i+1), n(i+1), and s(i+1),

wherein after said processing the N feedback entries, the database comprises k(N+1), n(N+1), and s(N+1).

29. The process of claim 28, said method comprising, as performed by the feedback module, synchronizing content of the database with the vendor, said synchronizing comprising sending to the vendor: (E_{ki} , H_{ni}, i = M, …, N) and E(k(N+1), n(N+1)), wherein 1 $\leq$M $\leq$N.

30. The process of claim29, wherein M=1.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 235
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

31. The process of claim 29, wherein M>1.

32. The process of claim 26, wherein a communication network is disposed between the end user machine and the vendor, wherein an application firewall is disposed between the end user machine and the communication network, and wherein the method further comprises permitting the feedback module to access the communication network, said permitting being controlled by the application firewall.

33. The process of claim 32, wherein the method further comprises preventing the software from accessing the communication network, said preventing being controlled by the application firewall.

34. The process of claim 32, wherein the communication network comprises the Internet.

35. The process of claim 26, wherein the identification tag is selected from the group consisting of a serial number of the software, a version number of the software and a combination of the serial number of the software and the version number of the software.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 236
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

Abstract of the Disclosure

A method and system for processing feedback entries received from software provided by a vendor to an end user machine. The end user machine includes the software, a feedback module, and a database. The feedback module: generates a secret key k(0) and makes the key k(0) known to both the vendor and a user of the software; generates a secret key n(0) and makes the key n0) known to the vendor but not to but not to the user; generates a secret key s(0) and makes the key s(0) known to the user but not to the vendor; generates an encryption E_{k0} of an identification tag using the key (k(0); generates a parameter H_{n0} such that H_{n0} = Hash(n(0) || E_{k0}); generates a parameter H_{s0} such that H_{s0} = Hash(s(0) || E_{k0}); sends E_{k0}, H_{n0}, and H_{s0} to the database; and sends E_{k0} and H_{s0} to the vendor.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 237
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

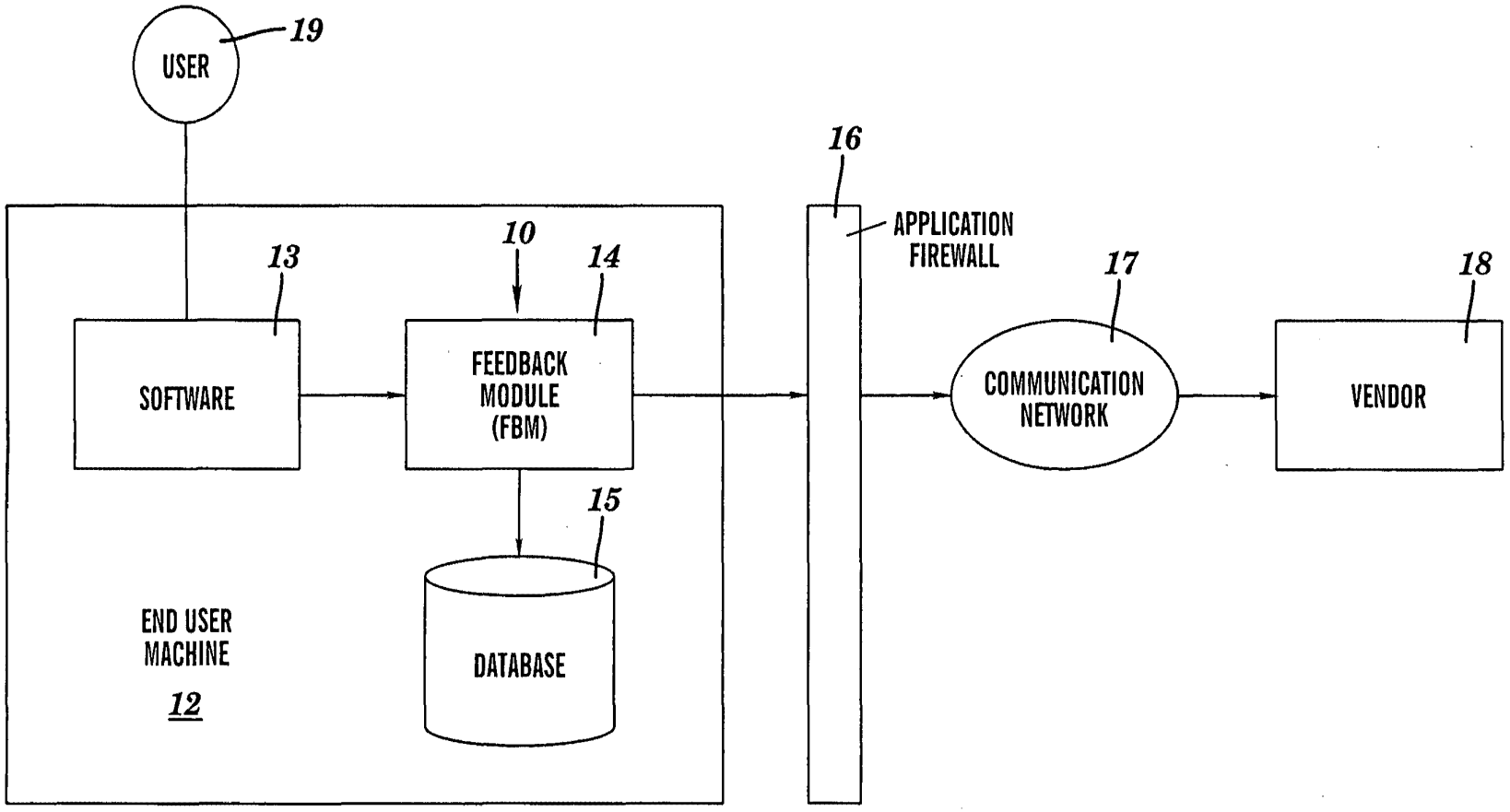
USER
19
16
APPLICATION
FIREWALL
10
13
14
17
18
SOFTWARE
FEEDBACK
MODULE
(FBM)
COMMUNICATION
NETWORK
VENDOR
15
END USER
MACHINE
12
DATABASE

FIG. 1

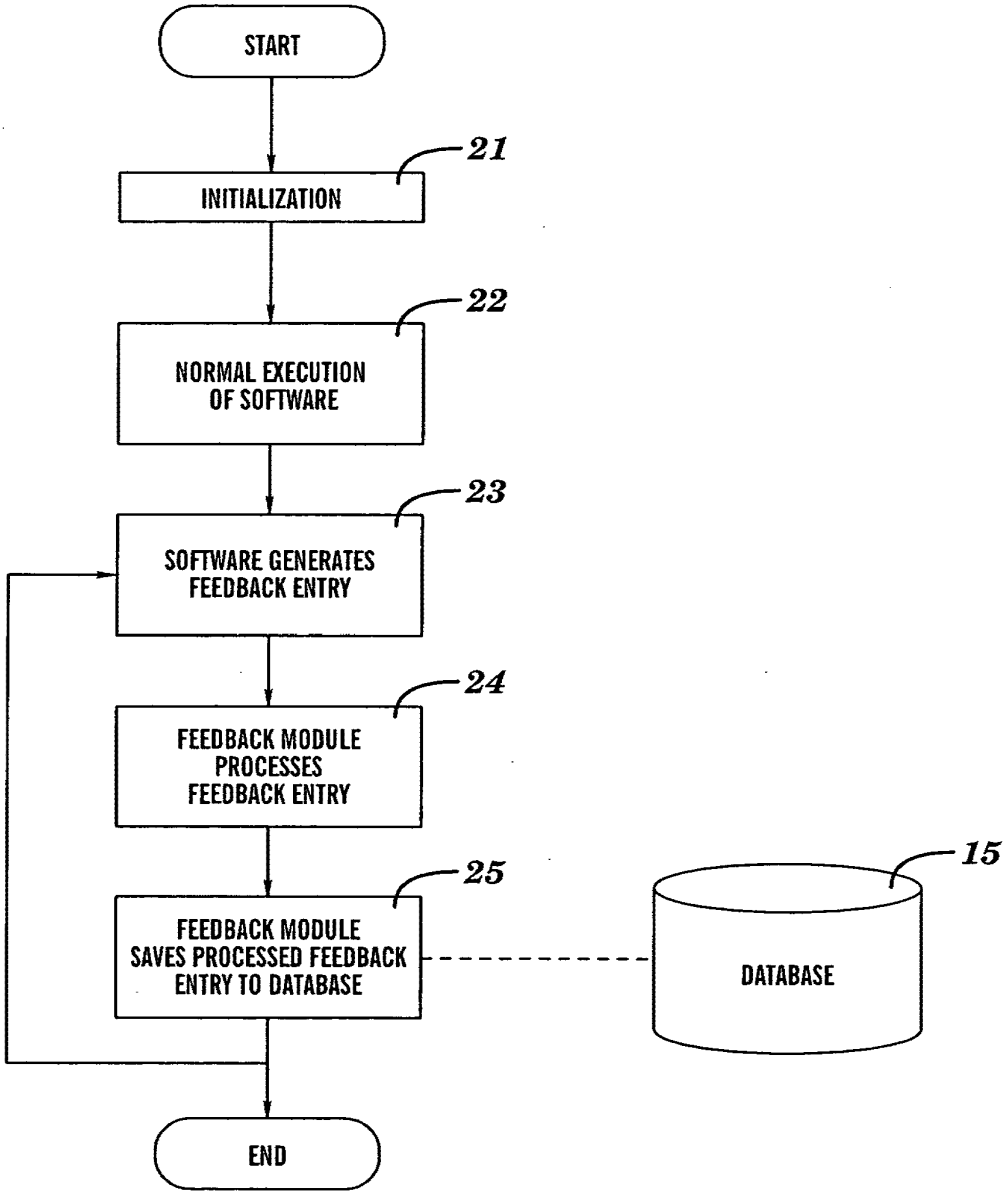
START
21
INITIALIZATION
22
NORMAL EXECUTION OF SOFTWARE
23
SOFTWARE GENERATES FEEDBACK ENTRY
24
FEEDBACK MODULE PROCESSES FEEDBACK ENTRY
25
FEEDBACK MODULE SAVES PROCESSED FEEDBACK ENTRY TO DATABASE
15
DATABASE
END

FIG. 2

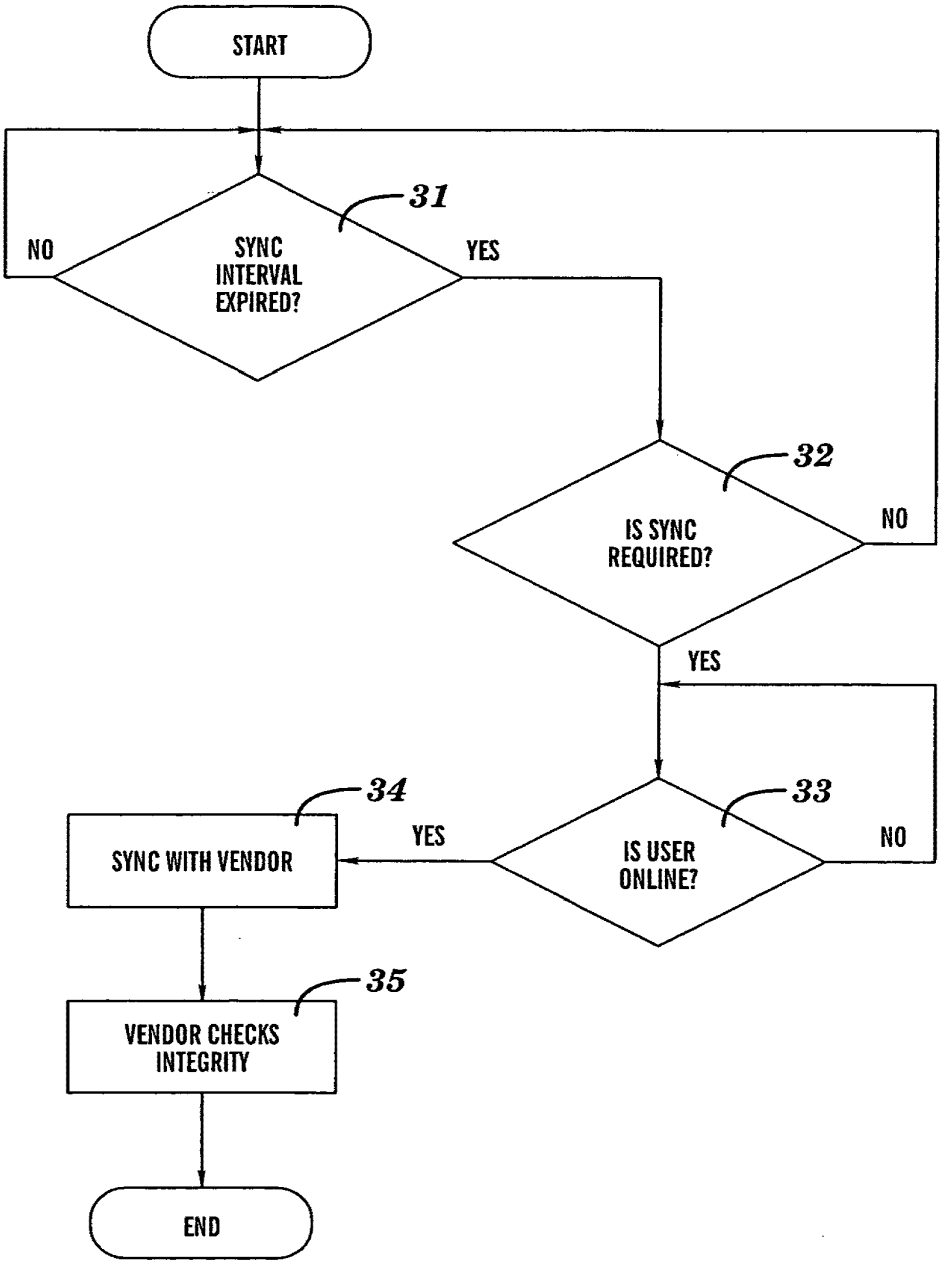
START
31
SYNC INTERVAL EXPIRED?
NO
YES
32
IS SYNC REQUIRED?
NO
YES
33
IS USER ONLINE?
YES
NO
34
SYNC WITH VENDOR
35
VENDOR CHECKS INTEGRITY
END

FIG. 3

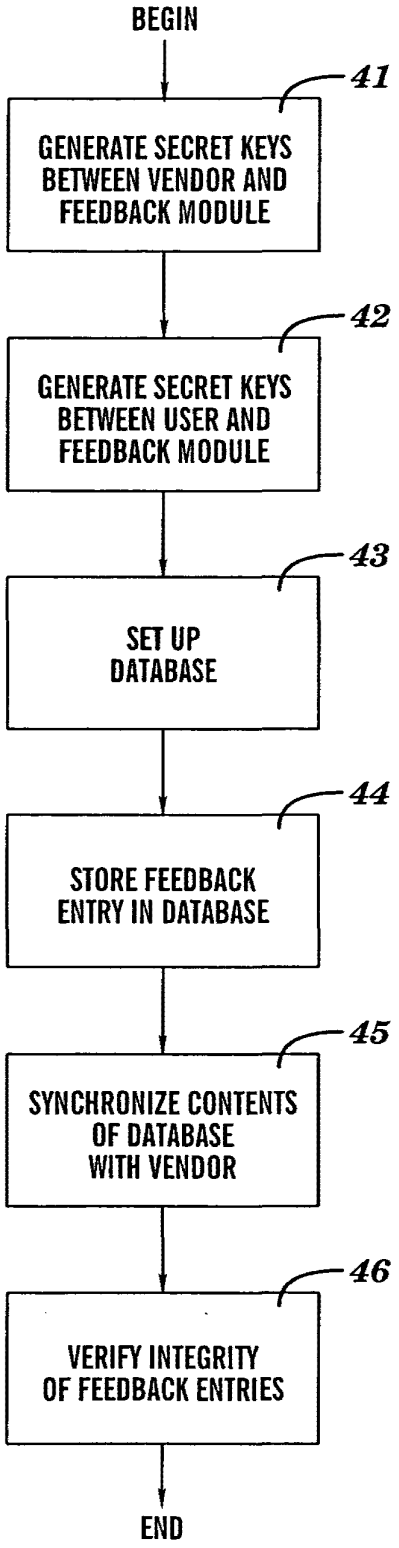
BEGIN
41
GENERATE SECRET KEYS BETWEEN VENDOR AND FEEDBACK MODULE
42
GENERATE SECRET KEYS BETWEEN USER AND FEEDBACK MODULE
43
SET UP DATABASE
44
STORE FEEDBACK ENTRY IN DATABASE
45
SYNCHRONIZE CONTENTS OF DATABASE WITH VENDOR
46
VERIFY INTEGRITY OF FEEDBACK ENTRIES
END

FIG. 4

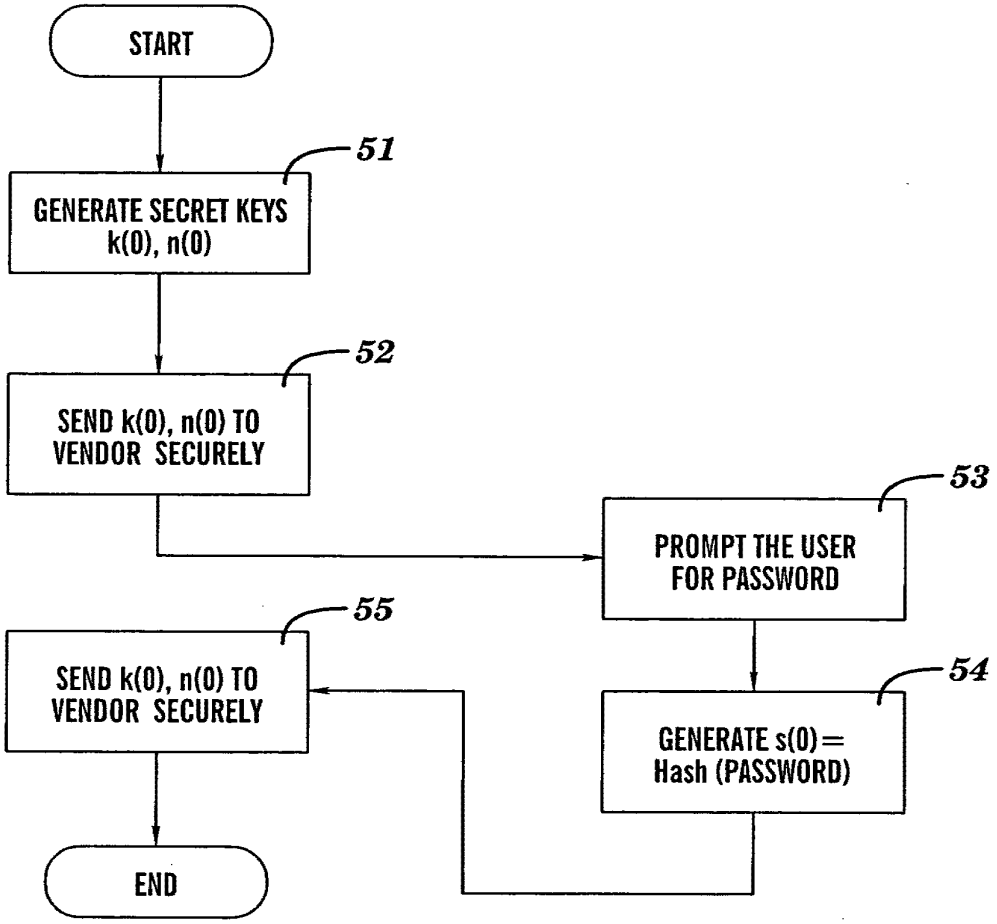
START
51
GENERATE SECRET KEYS k(0), n(0)
52
SEND k(0), n(0) TO VENDOR SECURELY
53
PROMPT THE USER FOR PASSWORD
54
GENERATE s(0) = Hash (PASSWORD)
55
SEND k(0), n(0) TO VENDOR SECURELY
END

FIG. 5

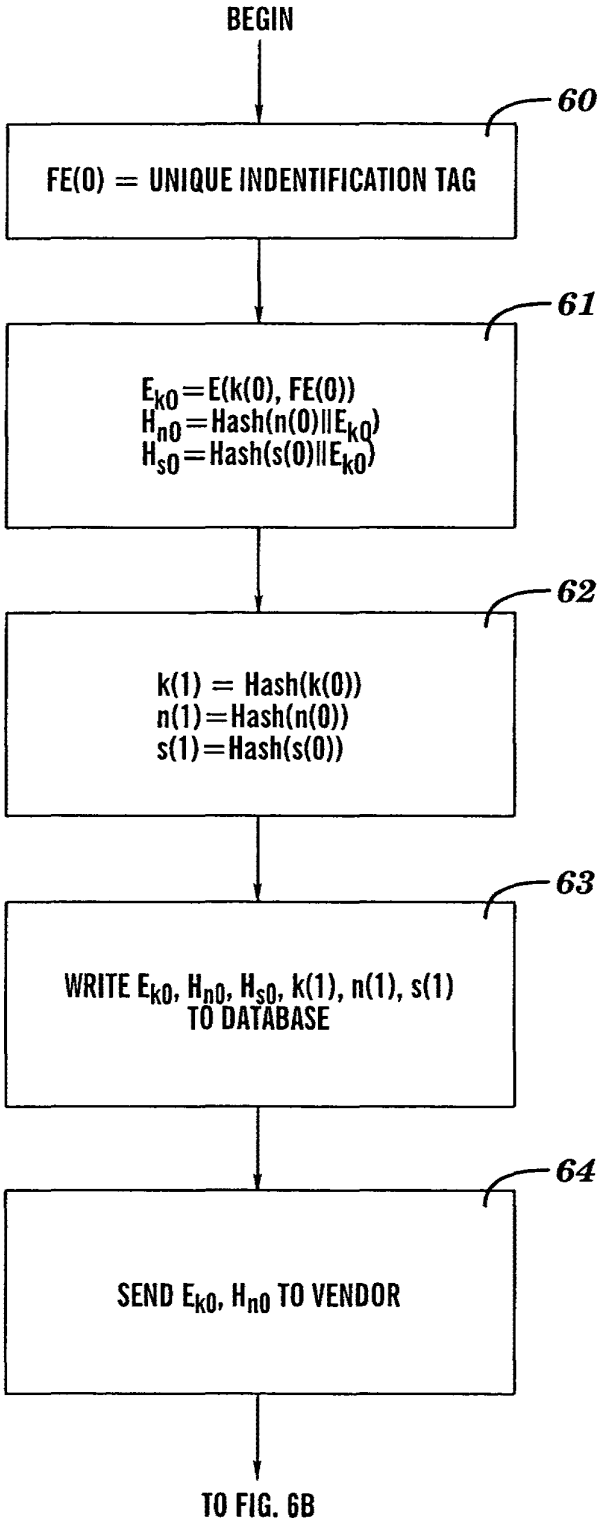
BEGIN
60
FE(0) = UNIQUE INDENTIFICATION TAG
61
E_{k0}=E(k(0), FE(0))
H_{n0}=Hash(n(0)||E_{k0})
H_{s0}=Hash(s(0)||E_{k0})
62
k(1) = Hash(k(0))
n(1)=Hash(n(0))
s(1)=Hash(s(0))
63
WRITE E_{k0}, H_{n0}, H_{s0}, k(1), n(1), s(1)
TO DATABASE
64
SEND E_{k0}, H_{n0} TO VENDOR
TO FIG. 6B

FIG. 6A

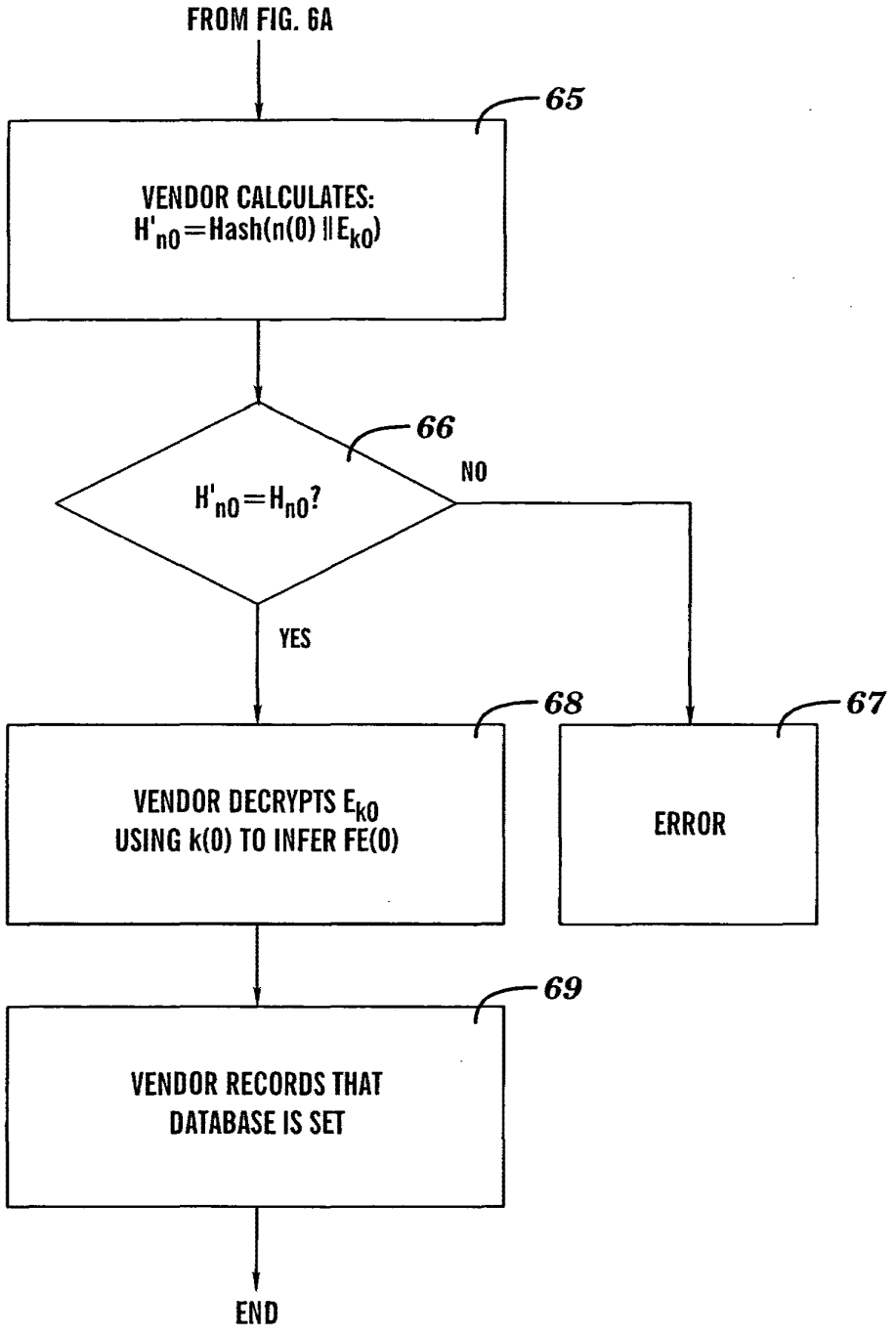
FROM FIG. 6A
65
VENDOR CALCULATES:
H'n0=Hash(n(0) || Ek0)
66
H'n0=Hn0?
NO
YES
68
VENDOR DECRYPTS Ek0
USING k(0) TO INFER FE(0)
67
ERROR
69
VENDOR RECORDS THAT
DATABASE IS SET
END

FIG. 6B

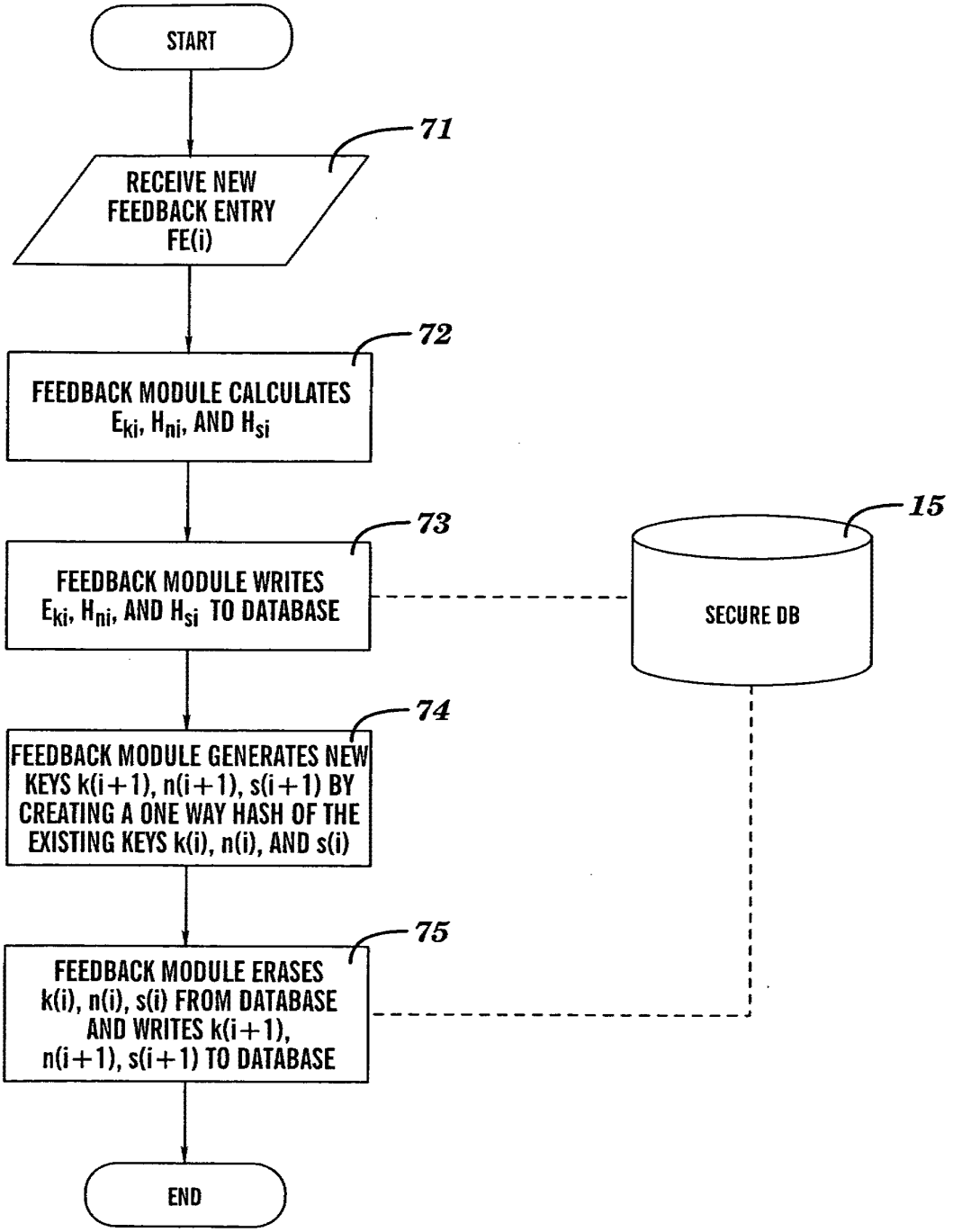
START
71
RECEIVE NEW FEEDBACK ENTRY FE(i)
72
FEEDBACK MODULE CALCULATES E_{ki}, H_{ni}, AND H_{si}
73
FEEDBACK MODULE WRITES E_{ki}, H_{ni}, AND H_{si} TO DATABASE
15
SECURE DB
74
FEEDBACK MODULE GENERATES NEW KEYS k(i+1), n(i+1), s(i+1) BY CREATING A ONE WAY HASH OF THE EXISTING KEYS k(i), n(i), AND s(i)
75
FEEDBACK MODULE ERASES k(i), n(i), s(i) FROM DATABASE AND WRITES k(i+1), n(i+1), s(i+1) TO DATABASE
END

FIG. 7

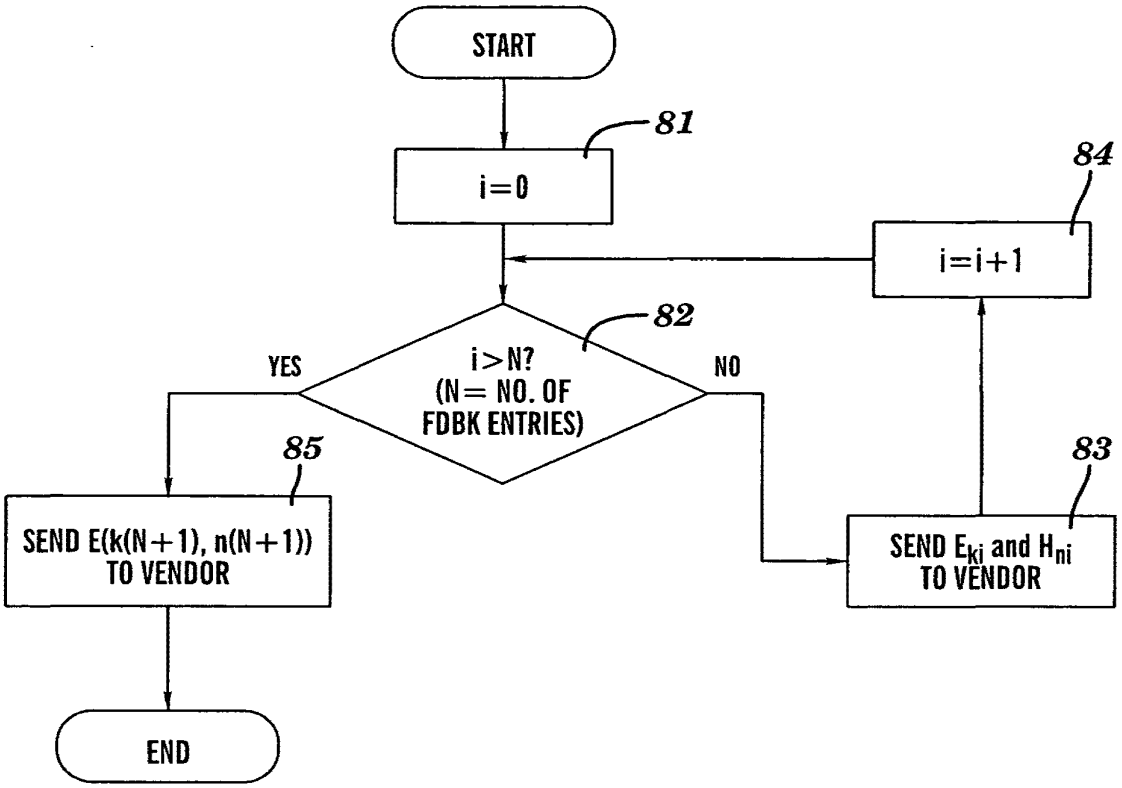
START
81
i=0
84
i=i+1
82
i>N?
(N= NO. OF
FDBK ENTRIES)
YES
NO
85
83
SEND E(k(N+1), n(N+1))
TO VENDOR
SEND E_{ki} and H_{ni}
TO VENDOR
END

FIG. 8

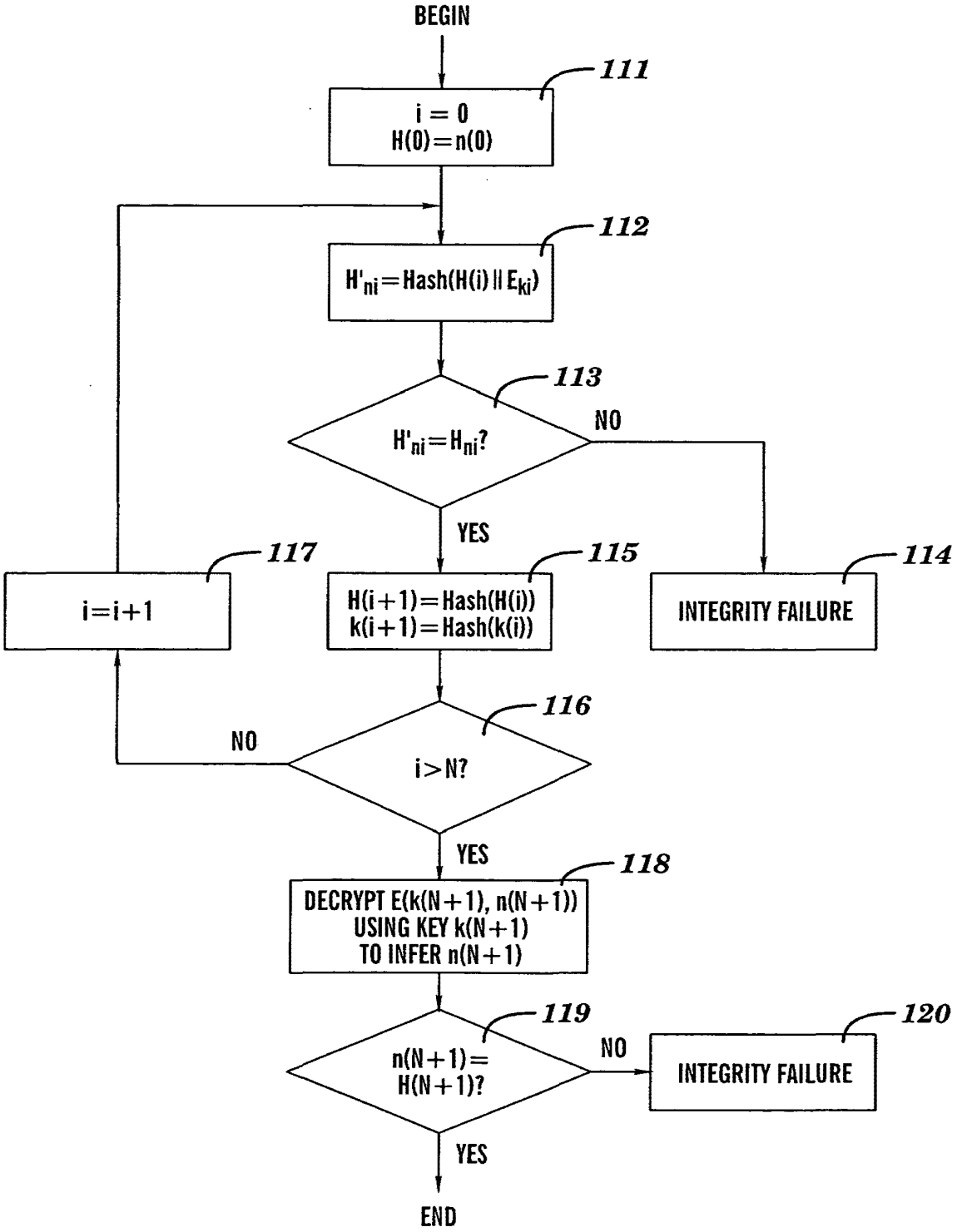
BEGIN
111
i = 0
H(0)=n(0)
112
H'ni=Hash(H(i) || Eki)
113
H'ni=Hni?
NO
YES
114
INTEGRITY FAILURE
115
H(i+1)=Hash(H(i))
k(i+1)=Hash(k(i))
117
i=i+1
116
i>N?
NO
YES
118
DECRYPT E(k(N+1), n(N+1))
USING KEY k(N+1)
TO INFER n(N+1)
119
n(N+1)=
H(N+1)?
NO
120
INTEGRITY FAILURE
YES
END

FIG. 9

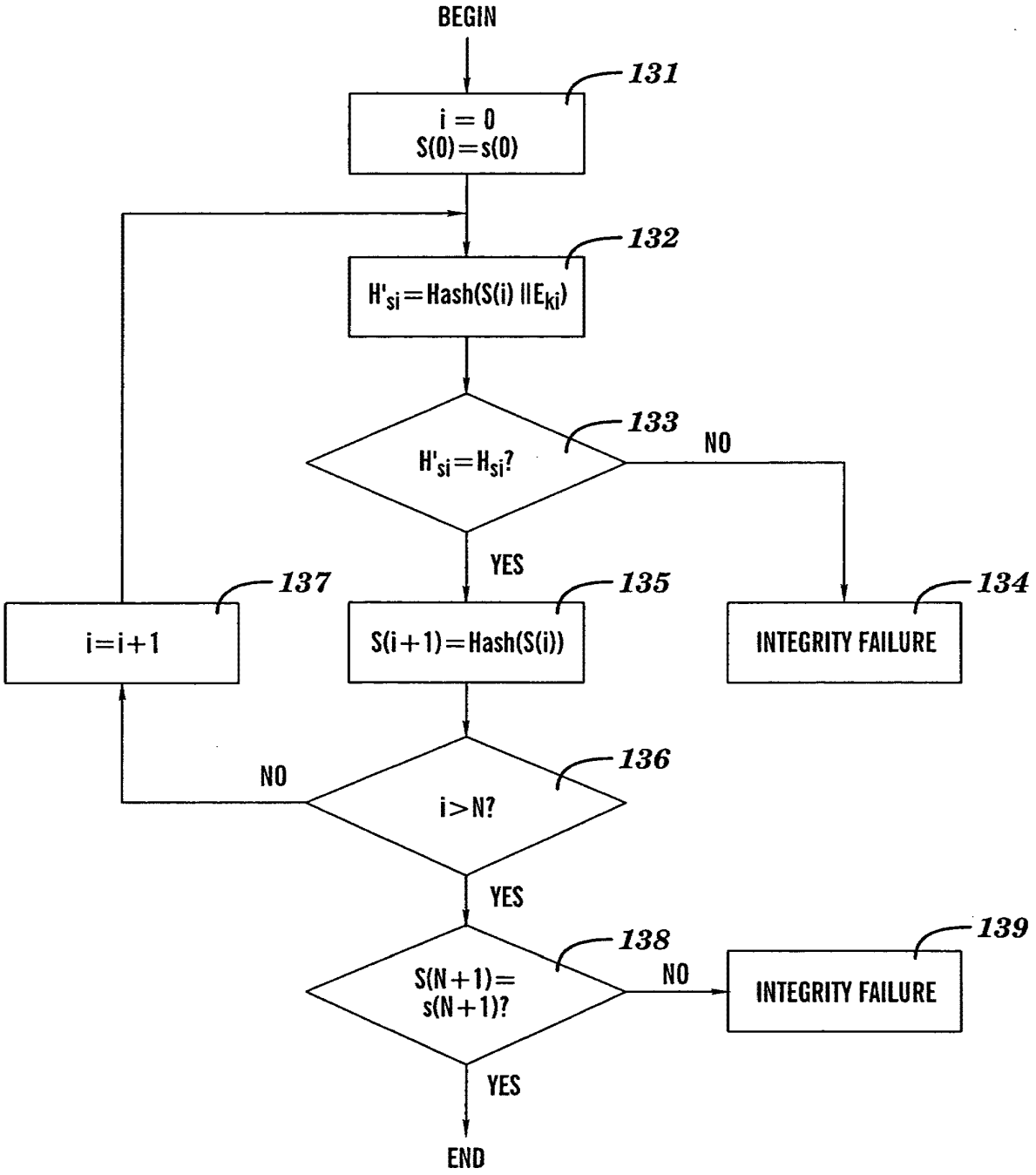
BEGIN
131
i = 0
S(0) = s(0)
132
H'si = Hash(S(i) ||Eki)
133
H'si = Hsi?
NO
YES
137
i = i + 1
135
S(i+1) = Hash(S(i))
134
INTEGRITY FAILURE
136
NO
i > N?
YES
138
S(N+1) =
s(N+1)?
NO
139
INTEGRITY FAILURE
YES
END

FIG. 10

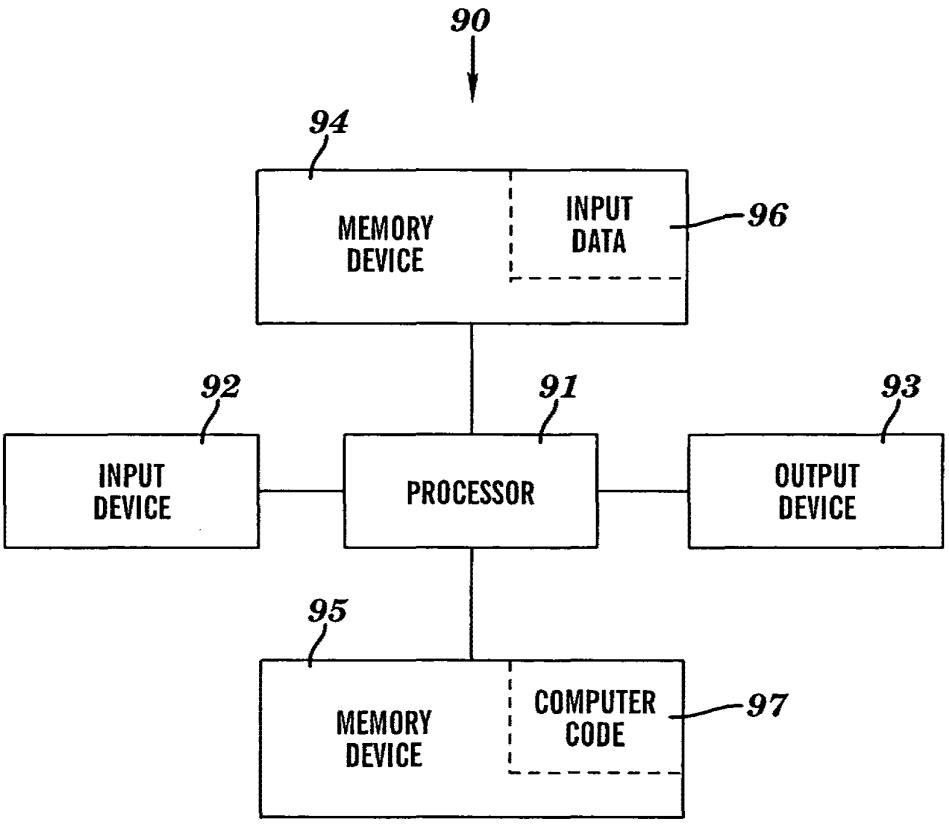
90
94
MEMORY DEVICE
INPUT DATA
96
92
91
93
INPUT DEVICE
PROCESSOR
OUTPUT DEVICE
95
MEMORY DEVICE
COMPUTER CODE
97

FIG. 11

Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my 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 PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

the specification of which (check one)

__X__ is attached hereto.

_____ was filed on _____ as Application Serial No. _____ and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above- identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, or plant breeder's rights certificate(s), or 356(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s):

Number	Country	Day/Month/Year	Priority Claimed

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 250
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

Application Serial No.: Filing Date

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

Prior U.S. Applications:

Serial No. Filing Date Status

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

All Attorneys/Agents associated with Customer No. 30449

Send all correspondence to: Customer No. 30449

Direct Telephone Calls to: Jack P. Friedman – (518) 220-1850

Executed by Inventor 1 of 1

(1) Inventor: **Vijil Enara Chenthamarakshan**

Signature: E. C. Vij 12/19/2005
Date

Residence: Enara, Muthalamada PO, Palghat, Kerala – 678507, India

Citizenship: Indian

Post Office Address: Same as Residence

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 252
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

PATENT APPLICATION SERIAL NO _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

01/09/2006 MAHMED1 00000035 090457 11325719

01 FC:1011	300.00	DA
02 FC:1111	500.00	DA
03 FC:1311	200.00	DA
04 FC:1202	750.00	DA

PTO-1556
(5/87)

U.S. Government Printing Office: 2002 — 460-247/69033

PTO/SB/06 (12-04)
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 Effective December 8, 2004

Application or Docket Number: 11/325,719

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	150.00		N/A	300.00
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	$250		N/A	$500
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	$100		N/A	$200
TOTAL CLAIMS (37 CFR 1.16(i))	35 minus 20 =	* 15	X$ 25 =		OR	X$50 =	750
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	* 0	X100 =			X200 =	–
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))			+180=			+360=	–
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1750

APPLICATION AS AMENDED – PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDI-TIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDI-TIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)	OR	RATE ($)	ADDI-TIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					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.

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.

Express Mail: ET808754613US

INFORMATION DISCLOSURE STATEMENT PURSUANT TO 37 C.F.R. §§1.97-1.99

PATENT APPLICATION

Applicant(s): Vijil Enara Chenthamarakshan Docket No.: IN920050028US1

FOR: **SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE**

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

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56 and pursuant to 37 C.F.R. §§1.97-1.99, Applicant(s) hereby notifies the U.S. Patent and Trademark Office of the documents listed on the attached Form PTO-1449. Applicant respectfully submits that all pending claims are patentable over the foregoing references, alone or in combination. The Examiner is requested to initial the enclosed Form PTO-1449 and return a copy thereof to the undersigned.

The submission of the listed documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant reserves the right to dispute any of the listed documents as prior art during examination. Further, Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application. Furthermore, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made or that no other material information may exist. This Information Disclosure Statement is being filed within three months of the filing date of the captioned patent application, and therefore no certification under 37 C.F.R. §1.97(e) or fee under 37 C.F.R. §1.17(p) is required.

Respectfully submitted,

Dated: 12/01/2005

By Jack P. Friedman
Jack P. Friedman
Reg. No. 44,688

Enclosures: PTO-1449

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	ATTY DOCKET NO. IN920050028US1	APPLICATION NO.
	APPLICANT(S) Vijil E. Chenthamarakshan	
	FILING DATE	GROUP ART UNIT

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		6,901,347	05/31/2005	Murray, *et al.*			
		6,842,752	01/11/2005	Itabashi, *et al.*			

U.S. PATENT APPLICATION PUBLICATIONS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2004/0210458	10/21/2004	Evans, *et al.*			
		2004/0167859	08/26/2004	Mirabella			
		2004/0139315	07/15/2004	Tokutani, *et al.*			
		2004/0034794	02/19/2004	Mayer, *et al.*			

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 256
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	ATTY DOCKET NO. IN920050028US1	APPLICATION NO.
	Vijil E. Chenthamarakshan	
	FILING	GROUP ART

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

U.S. PATENT APPLICATION PUBLICATIONS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2003/0133464	07/17/2003	Marejka, *et al.*			

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 257
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

Express Mail Label No. ET808754613US

22764 U.S. PTO
010506

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE

113010 U.S. PTO
11/325719
010506

and invented by:

Vijil Enara Chenthamarakshan
Assignee Name: International Business Machines Corporation
Assignee Address: New Orchard Road
Armonk, NY 10504

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 33 pages and including the following:
   a. ☒ Descriptive Title of the Invention
   b. ☐ Cross References to Related Applications *(if applicable)*
   c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   d. ☐ Reference to Sequence Listing, a Table, or a Computer Program Listing Appendix
   e. ☒ Background of the Invention
   f. ☒ Brief Summary of the Invention
   g. ☒ Brief Description of the Drawings *(if filed)*
   h. ☒ Detailed Description
   i. ☒ Claim(s) as Classified Below
   j. ☒ Abstract of the Disclosure

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 258
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

P01ULRG/REV09

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
   a. ☒ Formal Number of Sheets 12
   b. ☐ Informal Number of Sheets _____
4. ☒ Oath or Declaration
   a. ☒ Newly executed *(original or copy)* ☐ Unexecuted
   b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
   c. ☒ With Power of Attorney ☐ Without Power of Attorney
   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ CD ROM or CD-R in duplicate, large table or Computer Program (Appendix)
7. ☐ Application Data Sheet (See 37 CFR 1.76)
8. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statement(s) Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

9. ☐ Assignment Papers *(cover sheet & document(s))*
10. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
11. ☐ English Translation Document *(if applicable)*
12. ☒ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)* (2)
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☒ Certificate of Mailing
    ☐ First Class ☒ Express Mail *(Specify Label No.)*: ET808754613US

Security First Innovations, LLC, Exhibit 2014
P010LRG/REV09
Page 2014 - 259
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

Accompanying Application Parts (Continued)

17. ☐ Additional Enclosures *(please identify below):*

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

18. ☐ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

19. ☐ Other:

Security First Innovations, LLC, Exhibit 2014
Page 2014 - 260
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
IN920050028US1

Total Pages in this Submission
4

Fee Calculation and Transmittal

CLAIMS AS FILED						
For	**#Filed**	**#Allowed**	**#Extra**		**Rate**	**Fee**
Total Claims	35	- 20 =	15	x	$50.00	$750.00
Indep. Claims	3	- 3 =	0	x	$200.00	$0.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
Total # of Pages in Specification		33	**Total # of Drawing Sheets**		12	
Total # of Sheets	45				**Application Size Fee**	$0.00
					Basic Fee	$300.00
					Search Fee	$500.00
					Examination Fee	$200.00
OTHER FEE *(specify purpose)*						$0.00
					TOTAL FILING FEE	$1,750.00

☐ A check in the amount of to cover the filing fee is enclosed.

☒ The Director is hereby authorized to charge and credit Deposit Account No. **09-0457(IBM)** as described below.

- ☒ Charge the amount of **$1,750.00** as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

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

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.

Signature

Dated: 1/3/06

Customer Number: **30449**

cc:

William H. Steinberg
Reg. No. 28,540
IBM Corporation
IP Law Dept.
IQOA/040-3
1701 North St.
Endicott, NY 13760

Security First Innovations, LLC, Exhibit 2014
P01ULRG/REV09
Page 2014 - 261
IPR2025-01200, Intl. Bus. Machs. Corp. v. Security First Innovations, LLC

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10) Applicant(s): **Vijil Enara Chenthamarakshan**			Docket No. **IN920050028US1**	
Application No.	Filing Date	Examiner	Customer No. **30449**	Group Art Unit

Invention: **SYSTEM AND METHOD FOR PROCESSING FEEDBACK ENTRIES RECEIVED FROM SOFTWARE**

I hereby certify that the following correspondence:

Patent application and corresponding paperwork and IDS

(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

1/05/06
(Date)

Colleen Bulman
(Typed or Printed Name of Person Mailing Correspondence)

Colleen Bulman
(Signature of Person Mailing Correspondence)

ET808754613US
("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.