

EXHIBIT A



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

74877 7590 12/20/2010
 King and Spalding LLP
 1700 Pennsylvania Ave, NW
 Suite 200
 Washington, DC 20006

| | |
|-------------------------|--------------|
| EXAMINER | |
| WILLIAMS, JEFFERY L | |
| ART UNIT | PAPER NUMBER |
| 2437 | |
| DATE MAILED: 12/20/2010 | |

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | FIN0001CON1CIP3CIP1 | 5071 |

TITLE OF INVENTION: METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS FOR DESKTOP COMPUTERS

| APPLN. TYPE | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE |
|----------------|--------------|---------------|---------------------|----------------------|------------------|------------|
| nonprovisional | NO | \$1510 | \$300 | \$0 | \$1810 | 03/21/2011 |

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

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

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

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

If the SMALL ENTITY is shown as NO:

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

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.

74877 7590 12/20/2010

King and Spalding LLP
 1700 Pennsylvania Ave, NW
 Suite 200
 Washington, DC 20006

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. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | FIN0001CON1CIP3CIP1 | 5071 |

TITLE OF INVENTION: METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS FOR DESKTOP COMPUTERS

| APPLN. TYPE | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE |
|----------------|--------------|---------------|---------------------|----------------------|------------------|------------|
| nonprovisional | NO | \$1510 | \$300 | \$0 | \$1810 | 03/21/2011 |

| EXAMINER | ART UNIT | CLASS-SUBCLASS |
|---------------------|----------|----------------|
| WILLIAMS, JEFFERY L | 2437 | 726-025000 |

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

Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

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

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1 _____

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

_____ 3 _____

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

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

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

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

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

Issue Fee

Publication Fee (No small entity discount permitted)

Advance Order - # of Copies _____

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

A check is enclosed.

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

The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | FIN0001CON1CIP3CIP1 | 5071 |
| 74877 | 7590 | 12/20/2010 | EXAMINER | |
| King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006 | | | WILLIAMS, JEFFERY L | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2437 | |
| DATE MAILED: 12/20/2010 | | | | |

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 837 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 837 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.

| Notice of Allowability | Application No. | Applicant(s) | |
|-------------------------------|------------------|--------------|--|
| | 11/009,437 | RUBIN ET AL. | |
| | Examiner | Art Unit | |
| | JEFFERY WILLIAMS | 2437 | |

-- 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 9/15/2010.

2. The allowed claim(s) is/are 1-25.

3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some* c) None of the:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

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

4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
(a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
1) hereto or 2) to Paper No./Mail Date _____.
(b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

| | |
|--|---|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input checked="" type="checkbox"/> Interview Summary (PTO-413), Paper No./Mail Date <u>12/1/2010</u> . |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

Application/Control Number: 11/009,437
Art Unit: 2437

Page 2

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

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 a telephone interview with Dawn Marie Bey on 12/1/2010.

The application has been amended as follows:

13. (currently amended) A method for scanning content within a computer, comprising:
 receiving, at the computer, incoming content from the Internet on its destination to an Internet application;
 selectively diverting, by the computer, the received incoming content from its intended destination;
 scanning, by the computer, the selectively diverted incoming content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs,

Application/Control Number: 11/009,437
Art Unit: 2437

Page 3

1 and types of tokens comprising a punctuation type, an identifier type and a function
2 type; and
3 updating the database of parser and analyzer rules periodically to
4 incorporate new behavioral rules that are made available.

5

6 25. (currently amended) A computer-readable storage medium, the medium
7 excluding signals, storing program code for causing a computer to perform the steps of:
8 receiving incoming content from the Internet on its destination to an Internet
9 application;

10 selectively diverting the received incoming content from its intended destination;
11 scanning the selectively diverted incoming content to recognize potential exploits
12 therewithin, based on a database of parser and analyzer rules corresponding to
13 computer exploits, computer exploits being portions of program code that are malicious,
14 wherein the parser and analyzer rules describe exploits as patterns of types of tokens,
15 tokens being program code constructs, and types of tokens comprising a punctuation
16 type, an identifier type and a function type;

17 and updating the database of parser and analyzer rules periodically to
18 incorporate new parser and analyzer rules that are made available.

19

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

21 The prior art fails to disclose the features, as found recited in combination with
22 remaining claim limitations, of "*scanning, by the computer, the selectively diverted*
23 *incoming content to recognize potential computer exploits therewithin, based on a*

Application/Control Number: 11/009,437
Art Unit: 2437

Page 4

1 *database of parser and analyzer rules corresponding to computer exploits, computer*
2 *exploits being portions of program code that are malicious, wherein the parser and*
3 *analyzer rules describe computer exploits as patterns of types of tokens, tokens being*
4 *program code constructs, and types of tokens comprising a punctuation type, an*
5 *identifier type and a function type”.*

6 Any comments considered necessary by applicant must be submitted no later
7 than the payment of the issue fee and, to avoid processing delays, should preferably
8 accompany the issue fee. Such submissions should be clearly labeled “Comments on
9 Statement of Reasons for Allowance.” Any inquiry concerning this communication or
10 earlier communications from the examiner should be directed to JEFFERY WILLIAMS
11 whose telephone number is (571)272-7965. The examiner can normally be reached on
12 8:30-5:00.

13 If attempts to reach the examiner by telephone are unsuccessful, the examiner’s
14 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone
15 number for the organization where this application or proceeding is assigned is 571-
16 273-8300.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 5

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

10

11

12 /Jeffery Williams/
13 Examiner, Art Unit 2437

14

15 /Emmanuel L. Moise/
16 Supervisory Patent Examiner, Art Unit 2437

17

18

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|------------------------------|---|-------------------------------|
| In Re Patent Application of: |) | |
| |) | Examiner: Jeffrey L. Williams |
| Moshe Rubin |) | |
| Moshe Matitya |) | Art Unit: 2437 |
| Artem Melnick |) | |
| Shlomo Touboul |) | |
| Alexander Yermakov |) | |
| Amit Shaked |) | |
| |) | |
| Application No: 11/009,437 |) | |
| |) | |
| Filed: December 9, 2004 |) | |
| |) | |
| For: METHOD AND SYSTEM FOR |) | |
| ADAPTIVE RULE-BASED |) | |
| CONTENT SCANNERS FOR |) | |
| DESKTOP COMPUTERS |) | |
| |) | |

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

AMENDMENT AND RESPONSE TO OFFICE ACTION
UNDER 37 C.F.R. §1.111

Dear Examiner Williams:

In response to the Office Action dated June 15, 2010, applicants respectfully request that the above-identified application be amended as requested herein. A telephone interview has been scheduled for October 28, 2010 at 11:00 AM to discuss this application and the undersigned respectfully requests that if possible, the Examiner not take additional action on this application until after the interview.

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

1. (currently amended) A security system for scanning content within a computer, comprising:

a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer;

a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type;

a rule-based content scanner that communicates with said database of parser and analyzer rules, operatively coupled with said network interface, for scanning incoming content received by said network interface to recognize the presence of potential computer exploits therewithin;

a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content scanner; and

a rule update manager that communicates with said database of parser and analyzer rules, for updating said database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.

2. (previously presented) The security system of claim **1** wherein said database of parser and analyzer rules stores parser and analyzer rules in the form of pattern-matching engines.

3. (original) The security system of claim **2** wherein the pattern-matching engines are deterministic finite automata.

4. (original) The security system of claim 2 wherein the pattern-matching engines are non-deterministic finite automata.

5. (previously presented) The security system of claim 1 further comprising a content blocker, operatively coupled to said rule-based content scanner, for preventing incoming content having a computer exploit that was recognized by said rule-based content scanner from reaching its intended destination.

6. (previously presented) The system of claim 1 wherein the incoming content received from the Internet by said network interface is HTTP content.

7. (previously presented) The system of claim 1 wherein the incoming content received from the Internet by said network interface is HTTPS content.

8. (previously presented) The system of claim 1 wherein the incoming content received from the Internet by said network interface is FTP content

9. (previously presented) The system of claim 1 wherein the incoming content received from the Internet by said network interface is SMTP content

10. (previously presented) The system of claim 1 wherein the incoming content received from the Internet by said network interface is POP3 content

11. (original) The system of claim 1 wherein the destination Internet application is a web browser.

12. (original) The system of claim 1 wherein the destination Internet application is an e-mail client.

13. (currently amended) A method for scanning content within a computer, comprising:

receiving incoming content from the Internet on its destination to an Internet application;

selectively diverting the received incoming content from its intended destination;

scanning the selectively diverted incoming content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type; and

updating the database of parser and analyzer rules periodically to incorporate new behavioral rules that are made available.

14. (previously presented)The method of claim **13** wherein said database of parser and analyzer rules stores parser and analyzer rules in the form of pattern-matching engines.

15. (original) The method of claim **14** wherein the pattern-matching engines are deterministic finite automata.

16. (original) The method of claim **14** wherein the pattern-matching engines are non-deterministic finite automata.

17. (previously presented)The method of claim **13** further comprising preventing incoming content having a computer exploit that was recognized by said scanning from reaching its intended destination.

18. (previously presented)The method of claim **13** wherein the incoming content received from the Internet by said network interface is HTTP content.

19. (previously presented)The method of claim **13** wherein the incoming content received from the Internet by said network interface is HTTPS content.

20. (previously presented)The method of claim 13 wherein the incoming content received from the Internet by said network interface is FTP content

21. (previously presented)The method of claim 13 wherein the incoming content received from the Internet by said network interface is SMTP content

22. (previously presented)The method of claim 13 wherein the incoming content received from the Internet by said network interface is POP3 content

23. (original) The method of claim 13 wherein the destination Internet application is a web browser.

24. (original) The method of claim 13 wherein the destination Internet application is an e-mail client.

25. (currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving incoming content from the Internet on its destination to an Internet application;

selectively diverting the received incoming content from its intended destination;

scanning the selectively diverted incoming content to recognize potential exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe exploits as patterns of types of tokens, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type; and

updating the database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.

REMARKS

Applicants have carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicants have amended claims **1**, **13** and **25** to properly claim the present invention. No new matter has been added. Claims **1 - 25** are presented for examination.

Specification

On pages 2 and 3 of the Office Action, the Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter. Specifically, the Examiner has indicated that there is no support for “*patterns of types of tokens*”.

Applicants note that the appendix to the specification discloses that tokens are characterized into types. Thus, as defined on page 46,

IDENT “[A-Za-z[!underscore!][!dollar!]] [A-Za-z0-9[!underscore!][!dollar!]]*”,

a token consisting of a character a-z or a character A-Z or an underscore or a dollar sign, followed by zero or more of a character a-z or a character A-Z or a number 0 – 9 or an underscore or a dollar sign, is of type IDENT. Similarly, as defined on page 47,

INTEGER_DECIMAL “[0-9]+”,

a token consisting of one or more of the numbers 0 – 9, is of type INTEGER_DECIMAL; and

INTEGER_HEX “0[xX][0-9A-Fa-f]+”,

a token consisting of 0x or 0X followed by one or more of the numbers 0 - 9 or the characters A-F or the characters a-f, is of type INTEGER_HEX.

Applicants respectfully submit that patterns of types of tokens appear throughout the specification. Inter alia, at par. [0067], the specification recites

A parse tree ... uses parsing rules to identify groups of tokens as a single pattern.

Further, at par. [0085], the specification recites

For example, if a pattern “(IDENT) EQUALS NUMBER” is matched ... if a matched pattern is “(1 2 3) 4 5” ...

Further, at par. [0086], the specification recites

Reference is now made to FIG. 5, which is an illustration of a simple finite state machine ... for a pattern

(IDENT) <val==”foo” & match(*):Rule1>! <val==”bar”> EQUALS NUMBER

Specifically, the pattern of interest specifies either an IDENT token with value “foo” and that matches Rule1, or a List with value “bar”, followed by an EQUALS token and a NUMBER token.

Further, at par. [0094] the specification recites

For example, the pattern in the rule for FuncSig

(FUNCTION) (IDENT?) (List)

describes a keyword “function”, followed by zero or one IDENT tokens, and followed by a “List”. In turn, the pattern in the rule for List

(LPAREN) ((Expr (COMMA Expr)*)? (RPAREN)

describes an LPAREN token and an RPAREN token surrounding a list of zero or more Expr’s separated by COMMA tokens.

Further, at par. [0098], the specification recites

Referring back to the example above, the pattern

(IDENT) ASSIGNMENT IDENT <val==”screen”> DOT IDENT <val==”width”>

within the rule for ScrWidAssign describes a five-token pattern; namely (i) an IDENT token, followed by (ii) an ASSIGNMENT token, followed by (iii) an IDENT token that has a value equal to “screen”, followed by (iv) a DOT token, followed by (v) an IDENT token that has a value equal to “width”. Such a pattern ... corresponds to the example exploit listed above ...

Clearly items (i) – (v) above form a pattern of token types IDENT ASSIGNMENT IDENT DOT IDENT.

On page 3 of the Office Action, the Examiner has indicated that parsing rules for parsing of data into tokens, and analysis rules for analyzing the meaning of patterns of tokens are known concepts. Applicants respectfully submit that a point of novelty

of the claimed invention is describing and recognizing computer exploits from patterns of types of tokens, which is not a known concept.

Claim Rejections – 35 USC §112

On pages 3 and 4 of the Office Action, the Examiner has rejected claims **1 – 25** under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Applicants respectfully submit that the amended claims are supported in the original specification, as indicated above.

On pages 4 and 5 of the Office Action, the Examiner has rejected claims **1 – 25** under 35 U.S.C. §112, second paragraph, as being indefinite. Moreover, the Examiner has indicated that applicants point only to portions of the specification that describe what is standard and known prior art teaching for parsing and analyzing languages according to parsing rules and analyzing rules. Applications respectfully submit that the specification teaches recognition and detection of computer exploits from patterns of types of tokens, which is not standard and known prior art.

Claims Rejections - 35 USC §§102 and 103

On pages 5 – 7 of the Office Action, the Examiner has rejected claims **1, 2, 5, 6, 8 – 13, 17, 18 and 20 – 25** under 35 U.S.C. §102(e) as being anticipated by Freund, U.S. Patent No. 5,987,611 (“Freund”).

On pages 7 and 8 of the Office Action, the Examiner has rejected claims **3, 4, 7, 14 – 16 and 19** under 35 U.S.C. §103(a) as being unpatentable over Freund.

The rejections of claims **1 – 25** on pages 5 - 8 of the Office Action will now be dealt with specifically.

As to amended independent claim **1** for a security system, applicant respectfully submits that the limitations in claim **1** of

*“a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as **patterns of types of tokens**, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type”, and*

*“a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for **selectively diverting incoming content** from its intended destination to said rule-based content scanner”*

are neither shown nor suggested in Freund.

On page 9 of the Office Action, the Examiner has indicated that Freund teaches parsing data into recognizable tokens, wherein the tokens are not the same tokens and are distinct from one another. The Examiner is citing “*tokens*” in rejecting the claim limitations of “*patterns of types of tokens*”. Applicants wish to point out that the phrases “tokens” and “patterns of types of tokens” have different meanings. In particular, as used in the subject specification, “types of tokens” refers to a categorization of tokens into types. A “type” is a category. For example, the constructs APPLET, OBJECT, EMBED, SCRIPT, HREF and IMAGE are distinct tokens; yet they are all of the same type IDENT. Similarly, the constructs 0x01, 0XC33, 0xGB and 0X24AD3 are distinct tokens; yet they are all of the same type INTEGER_HEX.

Types of tokens disclosed in the subject specification include inter alia identifier tokens (say, type TYPE1), assignment tokens (say, type TYPE2), and punctuation tokens (say, type TYPE3). A pattern of types of tokens is, e.g., a pattern TYPE1 TYPE2 TYPE1 TYPE3 TYPE1; meaning, a token of type TYPE1 followed by a token of type TYPE2 followed by a token of type TYPE1 followed by a token of type TYPE3 followed by a token of type TYPE1; e.g., an identifier token followed by an assignment token followed by an identifier token followed by a punctuation token followed by an identifier token.

On page 9 of the Office Action, the Examiner has indicated that applicants fail to specifically explain how the recited language “*patterns of types of tokens*” distinguishes from the prior art. Applicants respectfully submit that the prior art does not relate to categorization of tokens into types, i.e., categories of tokens, and to description of computer exploits in terms of such categories. Moreover, the Examiner’s citations, e.g., Freund 23:44-55, 28:14-16 and 29:54 – 30:9 do not relate to patterns of types of tokens. Indeed, Freund 23:44-55 concerns types of Internet protocols, and not types of tokens. (An Internet protocol is not a token.) Freund 28:14 – 16 relates to filtering of rules. Freund 29:54 – 30:9 relates to specific tags (<APPLET>, <OBJECT>, <EMBED>, <SCRIPT>, <HREF> and <IMAGE>) and other “*syntax elements*” and “*HTML components*”. Applicants respectfully submit that tags, other syntax elements and HTML components may correspond to tokens, but they do not correspond to “*patterns of types*”.

Therefore, Freund does not teach categorization of tokens into types, nor description of computer exploits in terms of patterns of types of tokens.

In order to further clarify this distinction, applicants have amended claim **1** to include the limitation that types of tokens comprise a punctuation type, an identifier type and a function type.

In rejecting claim **1** on page 6 of the Office Action, the Examiner, referring to Freund, FIG. 3A:311, has indicated the Freund discloses a network traffic probe that selectively diverts incoming content from its intended destination to a rule-based content scanner. Applicants respectfully submit that elements 311a, 311b and 311c of Freund, FIG. 3A, are client-side monitors for monitoring Internet access (Freund 14:59-62), which do not divert incoming content to a content scanner. Indeed, Freund's client-side monitors limit Internet access; they do not divert incoming content to a content scanner.

In rejecting claim **2** on page 6 of the Office Action, the Examiner has cited Freund 29:54 – 30:10 as disclosing that the rules enable the driver or parser to operate according to a particular manner. Applicants respectfully submit that Freund does not disclose storing parser and analyzer rules in the form of pattern-matching engines, and that rules that operate according to a particular manner does not anticipate or render obvious rules stored in the form of pattern-matching engines. Examples of rules in the form of pattern matching engines are provided on pages 47 – 51 in the appendix of the original specification, and storing rules in the form of pattern matching engines is discussed at paragraphs [0071] – [0078] of the original specification with reference to FIGS. 4A and 4B.

Because claims **3 – 12** depend from claim **1** and include additional features, applicants respectfully submit that claims **2 - 12** are not anticipated or rendered obvious by Freund.

Accordingly claims **1 – 12** are deemed to be allowable.

As to amended independent method claim **13** and amended independent claim **25** for a computer-readable storage medium, applicants respectfully submit that the limitations in claims **13** and **25** of

“selectively diverting the received incoming content from its intended destination”, and

“scanning the selectively diverted incoming content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that

*are malicious, wherein the parser and analyzer rules describe computer exploits as **patterns of types of tokens**, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type”*

are neither shown nor suggested in Freund.

In rejecting claims **13** and **25** on page 7 of the Office Action, the Examiner has referenced his rejection of claim **1**, which cited Freund. As explained above, the claimed invention includes the limitation of patterns of types of tokens, which is not disclosed in Freund. The claimed invention also includes the limitation of selectively diverting incoming content, which is not disclosed in Freund.

Because claims **14 – 24** depend from claim **13** and include additional features, applicants respectfully submit that claims **14 - 24** are not anticipated or rendered obvious by Freund.

Accordingly claims **13 – 25** are deemed to be allowable.

Support for Amended Claims in Original Specification

Independent claims **1**, **13** and **25** have been amended to include the limitation that types of tokens include at least (i) a punctuation type, (ii) an identifier type and (iii) a function type. This limitation is supported in the original specification at least (i) by the various punctuation types of tokens defined on pages 46 and 47 (LBRACE, RBRACE, etc.), (ii) by the IDENT type of token defined on page 46, and (iii) by the FUNCTION type of token appearing on pages 29, 47 ad 48.

CONCLUSION

For the foregoing reasons, applicants respectfully submit that the applicable objections and rejections have been overcome and that the claims are in condition for allowance. The undersigned looks forward to discussing the response with the Examiner on October 28, 2010 at 11 AM. If any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account 50-4402.

Respectfully submitted,

Date: September 15, 2010

By: /Dawn-Marie Bey - 44,442/

King & Spalding LLP
1700 Pennsylvania Avenue
Suite 200
Washington DC 20006
(202) 626-8978

Dawn-Marie Bey
Registration No. 44,442



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. |
|---|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | FIN0001CON1CIP3CIP1 | 5071 |
| 74877 | 7590 | 06/15/2010 | EXAMINER | |
| King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006 | | | WILLIAMS, JEFFERY L | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2437 | |
| | | | NOTIFICATION DATE | DELIVERY MODE |
| | | | 06/15/2010 | ELECTRONIC |

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

dbey@KSLaw.com
 mblasik@kslaw.com
 jpaolella-bald@kslaw.com

Application/Control Number: 11/009,437
Art Unit: 2437

Page 3

1 *being program code constructs*" (e.g. see claim 1 and as similarly recited within
2 independent claims 13 and 25.

3 For example, the examiner notes that while the applicant appears to have
4 support for parser rules for defining and identifying "tokens" or sequences of characters
5 within a language and for analyzer rules for identifying the existence of patterns of
6 tokens (e.g. Specification, par. 53, 54, 63-65, appendix A), there is no support for the
7 present language of "patterns of types of tokens". The examiner respectfully points out
8 that language parsing and analyzing are basic and well known concepts within the art,
9 involving the parsing of character sequences into individual tokens and the analysis of
10 the token combinations or patterns for their meaning. It is respectfully noted that there
11 appears to be no support, nor reason for the applicant's present recitations. For the
12 purpose of examination, the examiner interprets such recitations as referencing the
13 parsing rules for parsing of data into tokens and analysis rules for analyzing the
14 meaning of patterns of tokens, according to the known meaning by those of ordinary
15 skill in the art.

16

17

Claim Rejections - 35 USC § 112

18

19

The following is a quotation of the first paragraph of 35 U.S.C. 112:

20

21

22

23

24

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 4

1 **Claims 1 – 25 are rejected under 35 U.S.C. 112, first paragraph, as failing to**
2 **comply with the written description requirement.** The claim(s) contains subject
3 matter which was not described in the specification in such a way as to reasonably
4 convey to one skilled in the relevant art that the inventor(s), at the time the application
5 was filed, had possession of the claimed invention. Applicant has not pointed out where
6 the new (or amended) claim is supported, nor does there appear to be a written
7 description of the claim limitations in the application as filed (see above objection to the
8 specification).

9

10 **The following is a quotation of the second paragraph of 35 U.S.C. 112:**

11 The specification shall conclude with one or more claims particularly pointing out and distinctly
12 claiming the subject matter which the applicant regards as his invention.

13

14 **Claims 1 – 25 are rejected under 35 U.S.C. 112, second paragraph, as being**
15 **indefinite for failing to particularly point out and distinctly claim the subject**
16 **matter which applicant regards as the invention.**

17 Regarding claims 1 – 25, the examiner notes that they comprise recitations of
18 “patterns of types of tokens”. Such recitations depart from the recitations found within
19 the applicant's disclosure and are not standard among those of ordinary skill in the art.
20 Furthermore, in argument for such recitations, the applicant points only to portions of
21 the specification describing what is standard and known prior art teaching for parsing
22 and analyzing language according to parsing rules and analyzing rules. Thus, the
23 examiner notes that such recitations as they are distinctly recited render the scope of
24 the claims unclear. For the purpose of examination the examiner interprets such

Application/Control Number: 11/009,437
Art Unit: 2437

Page 5

1 recitations as referencing the parsing rules for parsing of data into tokens (i.e.
2 sequences of characters) and analysis rules for analyzing the meaning of patterns of
3 tokens - such as disclosed by the applicant.

4 All depending claims are rejected by virtue of dependency.
5

6

7

Claim Rejections - 35 USC § 102

8

9 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that
10 form the basis for the rejections under this section made in this Office action:

11 A person shall be entitled to a patent unless –

12 (e) the invention was described in (1) an application for patent, published under section 122(b), by
13 another filed in the United States before the invention by the applicant for patent or (2) a patent
14 granted on an application for patent by another filed in the United States before the invention by the
15 applicant for patent, except that an international application filed under the treaty defined in section
16 351(a) shall have the effects for purposes of this subsection of an application filed in the United States
17 only if the international application designated the United States and was published under Article 21(2)
18 of such treaty in the English language.
19

20 **Claims 1, 2, 5, 6, 8 –12, 13, 17, 18, and 20 – 25 are rejected under 35**

21 **U.S.C. 102(e) as being anticipated by Freund, U.S. Patent, 5,987,611.**

22

23 Regarding claim 1, Freund discloses:

24 *a network interface, housed within a computer, for receiving incoming content*
25 *from the Internet on its destination to an Internet application running on the computer*
26 (Freund, fig. 2:220);

27 *a database of parser and analyzer rules corresponding to computer exploits,*
28 *stored within the computer (Fruend, fig. 5:570), computer exploits being portions of*

Application/Control Number: 11/009,437
Art Unit: 2437

Page 6

1 *program code that are potentially malicious (Fruend, 29:54 – 30:9), wherein the parser*
2 *and analyzer rules describe computer exploits as patterns of types of tokens, tokens*
3 *being program code constructs (Fruend, 23:44-55; 28:14-16; 29:54 – 30:9); a rule-*
4 *based content scanner that communicates with said database of parser and analyzer*
5 *rules, operatively coupled with said network interface, for scanning incoming content*
6 *received by said network interface to recognize the presence of potential computer*
7 *exploits therewithin (Fruend, 29:54-30:10); a network traffic probe, operatively coupled*
8 *to said network interface and to said rule-based content scanner, for selectively*
9 *diverting incoming content from its intended destination to said rule-based content*
10 *scanner (Fruend, fig. 3a:311);*

11 *and a rule update manager that communicates with said database of parser and*
12 *analyzer rules, for updating said database of parser and analyzer rules periodically to*
13 *incorporate new parser and analyzer rules that are made available (Fruend, 21:33-40).*

14

15 Regarding claim 2, Freund discloses:

16 *wherein said database of parser and analyzer rules stores parser and analyzer*
17 *rules in the form of pattern-matching engines (Fruend, 29:54-30:10). Herein, Freund*
18 *discloses that the rules enable the driver or parser to operate according to a particular*
19 *manner.*

20

21 Regarding claim 5, Freund discloses:

Application/Control Number: 11/009,437
Art Unit: 2437

Page 7

1 *a content blocker, operatively coupled to said rule-based content scanner, for*
2 *preventing incoming content having a potential computer exploit that was recognized by*
3 *said rule-based content scanner from reaching its intended destination (Freund, 15:22-*
4 *16:7).*

5

6 Regarding claims 6, 8 – 10, Freund discloses:

7 *wherein the incoming content received from the Internet by said network*
8 *interface is HTTP, FTP, SMTP, POP3 content (Freund, 23:44-55).*

9

10 Regarding claims 11 and 12, Freund discloses:

11 *wherein the destination Internet application is a web browser; wherein the*
12 *destination Internet application is an e-mail client (12:18-42).*

13

14 Regarding claims 13, 17, 18, 20 – 25, they are rejected, at least, for the same
15 reasons as claims 1, 5, 6, 8 – 12.

16

17 ***Claim Rejections - 35 USC § 103***

18

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

21

22

23

24

25

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

Application/Control Number: 11/009,437
Art Unit: 2437

Page 9

1 *Applicant argues or asserts essentially that:*

2 Examiner has cited Freund. The claimed invention, as amended, scans for
3 patterns of types of tokens, which is not disclosed in Freund. ... As such, Freund
4 makes it clear that the parsing comprises searching for designated tags. (Remarks, pg.
5 9, 10)

6

7 *Examiner respectfully responds:*

8 The examiner first respectfully notes that, while the applicant assumes a
9 particular characterization for the prior art, it is notable that the applicant fails to
10 specifically explain how the recited language “patterns of types of tokens” distinguishes
11 from the prior art. Essentially, applicant's remarks equate to only an allegation that the
12 claim recitations are novel in view of the prior art. Applicant's arguments fail to comply
13 with 37 CFR 1.111(b) because they amount to a general allegation that the claims
14 define a patentable invention without *specifically pointing out how the language of the*
15 *claims* patentably distinguishes them from the references.

16 Secondly, the examiner respectfully notes that the prior art teaches scanning for
17 patterns of types of tokens (e.g. see Freund, 23:44-55; 28:14-16; 29:54 – 30:9). Herein,
18 the prior art clearly parses data into recognizable tokens, wherein the tokens are not the
19 same tokens and are distinct from one another (i.e. different “types” of tokens), wherein
20 the tokens are analyzed according to their appearance within patterns identifiable as
21 malicious.

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 10

1 *Applicant argues or asserts essentially that:*

2 On page 3 of the Office Action, the Examiner has cited Freund 21:33 - 40, 23:44
3 - 55, 28:14 - 16 and 29:54 - 30:9 as teaching parser and analyzer rules for describing
4 computer exploits, Applicants respectfully submit that the rules described in Freund are
5 Internet access rules, and are not for rules for describing computer exploits (exploits
6 being portions of program code that are malicious), Indeed, FIGS, 7A - K of Freund step
7 the reader through creation of rules, several examples of which are shown including
8 rules for limiting what applications can do on the Internet, limiting what file types can be
9 downloaded, limiting the amount of time that users can spend on the Internet, etc,
10 (Freund/element 741 of FIG, 7B; also Abstract, 4:5 - 28, and 12:66- 13:22), Clearly,
11 these rules of Freund are not describing computer exploits, but instead are describing
12 rules to prevent abuse of Internet privileges by company personnel, to mitigate network
13 congestion, and to protect against downloading of viruses. (Remarks, pg. 10)

14

15 *Examiner respectfully responds:*

16 The examiner respectfully disagrees with the applicant's allegation and notes that
17 the prior art clearly discloses scanning content and using the rules to identify the
18 presence of exploits within the content that is deemed to be malicious (e.g. Freund,
19 29:45-30:10).

20

21

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 11

1 *Applicant argues or asserts essentially that:*

2 **Support for Amended Claims in Original Specification**

3 Independent claims 1, 13 and 25 have been amended to include the limitation of
4 parser and analyzer rules describing computer exploits as patterns of types of tokens.
5 This limitation is supported in the original specification at least by par. 66, 90, 91 and 97
6 - 103, and by the listing of Appendix A. (Remarks, pg. 11)

7

8 *Examiner respectfully responds:*

9 The examiner respectfully disagrees with the applicant's allegation that the
10 added claim recitations are supported within the applicant's original disclosure. For
11 example, the examiner notes that while the applicant appears to have support for parser
12 rules for defining and identifying "tokens" or sequences of characters within a language
13 and for analyzer rules for identifying the existence of patterns of tokens (e.g.
14 Specification, par. 53, 54, 63-65, appendix A), there is no support for the present
15 language of "patterns of types of tokens". The examiner respectfully points out that
16 language parsing and analyzing are basic and well known concepts within the art,
17 involving the parsing of character sequences into individual tokens and the analysis of
18 the token combinations or patterns for their meaning. It is respectfully noted that there
19 appears to be no support or reason for the applicant's present recitations.

20

21

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 12

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

See Notice of References Cited.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFERY WILLIAMS whose telephone number is (571)272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 13

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

10

11

12 /Jeffery Williams/
13 Examiner, Art Unit 2437

14

15 /Emmanuel L. Moise/
16 Supervisory Patent Examiner, Art Unit 2437

FIN0001CON1CIP3CIP1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|------------------------------|---|-------------------------------|
| In Re Patent Application of: |) | |
| |) | Examiner: Jeffrey L. Williams |
| Moshe Rubin |) | |
| Moshe Matitya |) | Art Unit: 2437 |
| Artem Melnick |) | |
| Shlomo Touboul |) | |
| Alexander Yermakov |) | |
| Amit Shaked |) | |
| |) | |
| Application No: 11/009,437 |) | |
| |) | |
| Filed: December 9, 2004 |) | |
| |) | |
| For: METHOD AND SYSTEM FOR |) | |
| ADAPTIVE RULE-BASED |) | |
| CONTENT SCANNERS FOR |) | |
| DESKTOP COMPUTERS |) | |
| |) | |

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

AMENDMENT AND RESPONSE TO OFFICE ACTION
UNDER 37 C.F.R. §1.116

Sir:

In response to the Office Action dated January 29,
2010, applicants respectfully request that the above-identified application
be amended as follows:

FIN0001CON1CIP3CIP1

PATENT

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

1. (currently amended) A security system for scanning content within a computer, comprising:

a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer;

a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as ~~logical combinations of~~ patterns of types of tokens, tokens being program code constructs;

a rule-based content scanner that communicates with said database of parser and analyzer rules, operatively coupled with said network interface, for scanning incoming content received by said network interface to recognize the presence of potential computer exploits therewithin;

a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content scanner; and

a rule update manager that communicates with said database of parser and analyzer rules, for updating said database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.

FIN0001CON1CIP3CIP1

PATENT

2. (previously presented) The security system of claim **1** wherein said database of parser and analyzer rules stores parser and analyzer rules in the form of pattern-matching engines.

3. (original) The security system of claim **2** wherein the pattern-matching engines are deterministic finite automata.

4. (original) The security system of claim **2** wherein the pattern-matching engines are non-deterministic finite automata.

5. (previously presented) The security system of claim **1** further comprising a content blocker, operatively coupled to said rule-based content scanner, for preventing incoming content having a computer exploit that was recognized by said rule-based content scanner from reaching its intended destination.

6. (previously presented) The system of claim **1** wherein the incoming content received from the Internet by said network interface is HTTP content.

7. (previously presented) The system of claim **1** wherein the incoming content received from the Internet by said network interface is HTTPS content.

8. (previously presented) The system of claim **1** wherein the incoming content received from the Internet by said network interface is FTP content

FIN0001CON1CIP3CIP1

PATENT

9. (previously presented) The system of claim **1** wherein the incoming content received from the Internet by said network interface is SMTP content

10. (previously presented) The system of claim **1** wherein the incoming content received from the Internet by said network interface is POP3 content

11. (original) The system of claim **1** wherein the destination Internet application is a web browser.

12. (original) The system of claim **1** wherein the destination Internet application is an e-mail client.

13. (currently amended) A method for scanning content within a computer, comprising:

receiving ~~currently amended~~ incoming content from the Internet on its destination to an Internet application;

selectively diverting the received ~~currently amended~~ incoming content from its intended destination;

scanning the selectively diverted ~~currently amended~~ incoming content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as ~~logical combinations of~~ patterns of types of tokens, tokens being program code constructs; and

FIN0001CON1CIP3CIP1

PATENT

updating the database of parser and analyzer rules periodically to incorporate new behavioral rules that are made available.

14. (previously presented) The method of claim **13** wherein said database of parser and analyzer rules stores parser and analyzer rules in the form of pattern-matching engines.

15. (original) The method of claim **14** wherein the pattern-matching engines are deterministic finite automata.

16. (original) The method of claim **14** wherein the pattern-matching engines are non-deterministic finite automata.

17. (previously presented) The method of claim **13** further comprising preventing incoming content having a computer exploit that was recognized by said scanning from reaching its intended destination.

18. (previously presented) The method of claim **13** wherein the incoming content received from the Internet by said network interface is HTTP content.

19. (previously presented) The method of claim **13** wherein the incoming content received from the Internet by said network interface is HTTPS content.

20. (previously presented) The method of claim **13** wherein the incoming content received from the Internet by said network interface is FTP content

FIN0001CON1CIP3CIP1

PATENT

21. (previously presented) The method of claim **13** wherein the incoming content received from the Internet by said network interface is SMTP content

22. (previously presented) The method of claim **13** wherein the incoming content received from the Internet by said network interface is POP3 content

23. (original) The method of claim **13** wherein the destination Internet application is a web browser.

24. (original) The method of claim **13** wherein the destination Internet application is an e-mail client.

25. (currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving incoming content from the Internet on its destination to an Internet application;

selectively diverting the received incoming content from its intended destination;

scanning the selectively diverted incoming content to recognize potential exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe exploits as ~~logical combinations of~~ types of tokens, tokens being program code constructs; and

FIN0001CON1CIP3CIP1

PATENT

updating the database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.

FIN0001CON1CIP3CIP1

PATENT

REMARKS

Applicants have carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicants have amended claims **1, 13** and **25** to properly claim the present invention. No new matter has been added. Claims **1 - 25** are presented for examination.

On pages 2 – 4 of the Office Action, the Examiner has rejected claims **1, 2, 5, 6, 8 – 13, 17, 18** and **20 – 25** under 35 U.S.C. §102(e) as being anticipated by Freund, U.S. Patent No. 5,987,611 (“Freund”).

On pages 4 and 5 of the Office Action, the Examiner has rejected claims **3, 4, 7, 14 – 16** and **19** under 35 U.S.C. §103(a) as being unpatentable over Freund.

Response to Examiner’s Arguments

The rejections of claims **1 – 25** on pages 2 - 5 of the Office Action will now be dealt with specifically.

As to amended independent claim **1** for a security system, applicant respectfully submits that the limitations in claim **1** of

“a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs”

is neither shown nor suggested in Freund.

FIN0001CON1CIP3CIP1

PATENT

Applicants have amended claim **1** to include the limitation of parser and analyzer rules describing computer exploits as patterns of types of tokens. Types of tokens include, e.g., identifier tokens of type TYPE1, assignment tokens of type TYPE2, and punctuation tokens of type TYPE3. Definitions of these types of tokens appear in the original specification at least at par. 66, 90 and 91, and in Appendix A on page 46. A pattern of types of tokens is, e.g., a pattern TYPE1 TYPE2 TYPE1 TYPE3 TYPE1 (meaning, a token of type TYPE1 followed by a token of type TYPE2 followed by a token of type TYPE1 followed by a token of type TYPE3 followed by a token of type TYPE1; e.g., an identifier token followed by an assignment token followed by an identifier token followed by a punctuation token followed by an identifier token). Definitions of these patterns appear in the original specification at least at par. 97 - 103 and in Appendix A on pages 49 - 52.

In rejecting claim **1** on page 3 of the Office Action, the Examiner has cited Freund. The claimed invention, as amended, scans for patterns of types of tokens, which is not disclosed in Freund. Specifically, Freund describes Internet access management that, inter alia, includes access rules that govern "a list of list of protocols or protocol components (such as Java Script™) that a user application can or cannot use" (Freund 4: 15 - 17). Freund describes interpreting protocol commands at 29:17 - 30:10, with reference to FIG. 12. In particular, with reference to step 1220 of FIG. 12, Freund states "At step 1220 the content driver parses the contents of "foo.html" and checks for the following components: (a) References to Java™, ActiveX and the like (<APPLET> or <OBJECT> tags); (b) References to Netscape style plug-ins (<EMBED> tag); (c) Imbedded scripts such as Java Script™, VBScript, and the like (<SCRIPT> tag); (d) References to other files or components

FIN0001CON1CIP3CIP1

PATENT

(*, or tags*); and (e) *Other syntax elements that are known or suspected to cause security or network problems.*" (Freund: 20:59 – 30:1). As such, Freund makes it clear that the parsing comprises searching for designated tags.

On page 3 of the Office Action, the Examiner has cited Freund 21: 33 – 40, 23: 44 – 55, 28:14 – 16 and 29:54 – 30:9 as teaching parser and analyzer rules for describing computer exploits. Applicants respectfully submit that the rules described in Freund are Internet access rules, and are not for rules for describing computer exploits (exploits being portions of program code that are malicious). Indeed, FIGS. 7A - K of Freund step the reader through creation of rules, several examples of which are shown including rules for limiting what applications can do on the Internet, limiting what file types can be downloaded, limiting the amount of time that users can spend on the Internet, etc. (Freund/ element 741 of FIG. 7B; also Abstract, 4: 5 – 28, and 12:66 – 13:22). Clearly, these rules of Freund are not describing computer exploits, but instead are describing rules to prevent abuse of Internet privileges by company personnel, to mitigate network congestion, and to protect against downloading of viruses.

Because claims **2 – 12** depend from claim **1** and include additional features, applicants respectfully submit that claims **2 - 12** are not anticipated or rendered obvious by Freund.

Accordingly claims **1 – 12** are deemed to be allowable.

As to amended independent method claim **13** and amended independent claim **25** for a computer-readable storage medium, applicants respectfully submit that the limitation in claims **13** and **25** of

"scanning the selectively diverted incoming content to recognize potential computer exploits therewithin, based on a database of

FIN0001CON1CIP3CIP1

PATENT

parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs"

is neither shown nor suggested in Freund.

In rejecting claim **13** and **25** on page 4 of the Office Action, the Examiner has referenced his rejection of claim **1**, which cited Freund. As explained above, the claimed invention, as amended, scans for patterns of types of tokens, which is not disclosed in Freund. Moreover, the rules described in Freund are Internet access rules, and not rules for describing computer exploits.

Because claims **14** – **24** depend from claim **13** and include additional features, applicants respectfully submit that claims **14** - **24** are not anticipated or rendered obvious by Freund.

Accordingly claims **13** – **25** are deemed to be allowable.

Support for Amended Claims in Original Specification

Independent claims **1**, **13** and **25** have been amended to include the limitation of parser and analyzer rules describing computer exploits as patterns of types of tokens. This limitation is supported in the original specification at least by par. 66, 90, 91 and 97 - 103, and by the listing of Appendix A.

FIN0001CON1CIP3CIP1

PATENT

CONCLUSION

The undersigned representative respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that the prosecution might be advanced by discussing the application with the undersigned representative, in person or over the telephone, we welcome the opportunity to do so. In addition, if any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account No. 504402.

Respectfully submitted,

Date: March 26, 2010
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4706
(202) 737-0500

By: /Eric L. Sophir, Reg. #48,499/
Eric L. Sophir
Registration No. 48,499



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. |
|---|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | FIN0001CON1CIP3CIP1 | 5071 |
| 74877 | 7590 | 01/29/2010 | EXAMINER | |
| King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006 | | | WILLIAMS, JEFFERY L | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2437 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 01/29/2010 | 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.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 2

1 **DETAILED ACTION**

2
3 Claims 1 – 25 are rejected.

4 This action is in response to the communication filed on 12/18/09.

5 All objections and rejections not set forth below have been withdrawn.

6
7 ***Claim Rejections - 35 USC § 102***

8
9 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that
10 form the basis for the rejections under this section made in this Office action:

11 A person shall be entitled to a patent unless –

12 (e) the invention was described in (1) an application for patent, published under section 122(b), by
13 another filed in the United States before the invention by the applicant for patent or (2) a patent
14 granted on an application for patent by another filed in the United States before the invention by the
15 applicant for patent, except that an international application filed under the treaty defined in section
16 351(a) shall have the effects for purposes of this subsection of an application filed in the United States
17 only if the international application designated the United States and was published under Article 21(2)
18 of such treaty in the English language.

19
20 **Claims 1, 2, 5, 6, 8 –12, 13, 17, 18, and 20 – 25 are rejected under 35**

21 **U.S.C. 102(e) as being anticipated by Freund, U.S. Patent, 5,987,611.**

22
23 Regarding claim 1, Freund discloses:

24 *a network interface, housed within a computer, for receiving incoming content*
25 *from the Internet on its destination to an Internet application running on the computer*

26 (Freund, fig. 2:220);

Application/Control Number: 11/009,437
Art Unit: 2437

Page 3

1 *a database of parser and analyzer rules corresponding to computer exploits,*
2 *stored within the computer (Fruend, fig. 5:570), computer exploits being portions of*
3 *program code that are potentially malicious (Fruend, 29:54 – 30:9), wherein the parser*
4 *and analyzer rules describe computer exploits as logical combinations of patterns of*
5 *program code constructs (Fruend, 23:44-55; 28:14-16; 29:54 – 30:9); a rule-based*
6 *content scanner that communicates with said database of parser and analyzer rules,*
7 *operatively coupled with said network interface, for scanning incoming content received*
8 *by said network interface to recognize the presence of potential computer exploits*
9 *therewithin (Fruend, 29:54-30:10); a network traffic probe, operatively coupled to said*
10 *network interface and to said rule-based content scanner, for selectively diverting*
11 *incoming content from its intended destination to said rule-based content scanner*
12 *(Fruend, fig. 3a:311);*

13 *and a rule update manager that communicates with said database of parser and*
14 *analyzer rules, for updating said database of parser and analyzer rules periodically to*
15 *incorporate new parser and analyzer rules that are made available (Fruend, 21:33-40).*

16

17 Regarding claim 2, Freund discloses:

18 *wherein said database of parser and analyzer rules stores parser and analyzer*
19 *rules in the form of pattern-matching engines (Fruend, 29:54-30:10). Herein, Freund*
20 *discloses that the rules enable the driver or parser to operate according to a particular*
21 *manner.*

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 5

1 invention was made to a person having ordinary skill in the art to which said subject matter pertains.
2 Patentability shall not be negated by the manner in which the invention was made.

3
4 **Claims 7 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable**
5 **over Freund, U.S. Patent, 5,987,611.**

6
7 Regarding claims 7 and 19, Freund discloses that the system is flexible so as to
8 support a plurality of protocols (Freund, 12:18-42). While Freund discloses supporting
9 existing protocols such as HTTP, Freund does not appear to explicitly state that the
10 system may support secure HTTP. However, it would have been obvious to one of
11 ordinary skill in the art to employ support for the secure HTTP because one of ordinary
12 skill in the art would have been motivated by increased flexibility of the system.

13
14 Regarding claims 3, 4, and 14 – 16, Freund discloses parsing means for pattern
15 matching, but does not appear to disclose DFA or NDFA. However, the examiner notes
16 that it was well known in the art for DFA and NDFA to be used as engines for pattern
17 matching (e.g. see admission by the applicant, Applicant's specification, par. 73).

18
19
20 ***Response to Arguments***

21
22 Applicant's arguments filed 12/18/09 have been fully considered but they are not
23 persuasive.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 6

1 *Applicant argues or asserts essentially that:*

2 ... Freund concerns monitoring outbound access to the Internet, whereas the
3 claimed invention concerns protection from inbound computer exploits. The title and
4 headings of Freund make it clear that Freund is primarily concerned about unauthorized
5 use of the Internet by company employees. Cf. the headings at 8:39 and col. 9:64, and
6 the example at 9:37-53. ...

7 ...

8 To further clarify this distinction, applicants have amended the claims to refer to
9 the content as incoming content.

10 ...

11 In rejecting claim 1 the Examiner has cited Freund 21:33-40 as disclosing "a rule
12 update manager ... for updating ... parser and analyzer rules ..." Applicants respectfully
13 submit that Freund fails to disclose parser and analyzer rules for scanning inbound
14 content. Instead, Freund describes a rules database for rules that define permitted
15 outbound Internet activity by a client machine. Cf. Freund 4:8-19, 9:37- 53 and 13:2-13.

16 ...

17 Additionally, the Examiner has cited Freund FIG. 5:570 as disclosing a database
18 of parser and analyzer rules corresponding to computer exploits. Applicants respectfully
19 submit that Freund fails to disclose a database of parser and analyzer rules for
20 scanning inbound content. Instead, database 570 stores rules which define permitted
21 outbound activity for a client machine. ...

22 **(Remarks, pg. 9-11)**

Application/Control Number: 11/009,437
Art Unit: 2437

Page 7

1

2 *Examiner respectfully responds:*

3 The examiner notes that the applicant appears to argue that the prior art does
4 not disclose scanning “inbound content”, but rather, only focuses on access to the
5 Internet, alleged to be “outbound access”. However, the examiner respectfully points
6 out that the applicant appears to be misinterpret the prior art. Specifically, the prior art
7 is concerned with monitoring Internet access, which of course includes the bidirectional
8 flow of content to and from the Internet. For example, even though a client might send
9 a request (i.e. “outbound”) to access content of the Internet (e.g. a web site), it would be
10 unable to access such content if that content were not sent from Internet and received
11 by the client (i.e. “inbound”). Freund clearly gives examples of monitoring and scanning
12 both outbound and inbound content associated with Internet access (e.g. Freund,
13 29:45-30:10).

14

15

16 *Applicant argues or asserts essentially that:*

17 ... Applicants respectfully submit that Freund fails to disclose such parser and
18 analyzer rules. Instead, Freund discloses drivers for monitoring different types of
19 outbound Internet access protocols made from a client machine. **(Remarks, pg. 12)**

20

21

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 8

1 *Examiner respectfully responds:*

2 The examiner respectfully notes that the applicant's argument appears to be
3 based upon the same rationale previously presented. Specifically, the applicant
4 focuses on the presumption that the prior art teaches only monitoring outbound internet
5 activity. However, the examiner notes that the applicant's remarks are found to be
6 unpersuasive for the reasons already noted, and maintains that the prior art discloses
7 parsing and analyzing "inbound content" (e.g. 29:54-30:10).

8

9 *Applicant argues or asserts essentially that:*

10 Additionally, the Examiner has cited Freund 29:54 - 30:9 as disclosing "*scanning*
11 *content ... to recognize the presence of potential computer exploits therewithin*".
12 Applicants wish to point out that computer exploits are defined within claim 1 as being
13 portions of program code that are malicious. Freund discloses recognizing components
14 of an HTML page, including JAVA TM applets, ActiveX controls, plug-ins, embedded
15 scripts and references to other files or components. However, Freund does not analyze
16 these components for the presence of computer exploits. Instead, Freund simply checks
17 the rules database to see if a component is permissible. As such, Freund is unable to
18 distinguish between a safe applet and a malicious applet. Freund simply allows or
19 blocks all applets. **(Remarks, pg. 12)**

20

21

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 9

1 *Examiner respectfully responds:*

2 The examiner points out that the claim recites scanning content so as to
3 recognize content that is potentially malicious. The claims fail to comprise any explicit
4 recitations regarding the handling of applets and the need distinguish between safe
5 applets and malicious applets. Thus, the examiner respectfully notes that the
6 applicant's assertion that Freund "is unable to distinguish between a safe applet and a
7 malicious applet" does not appear to be relevant.

8 Furthermore, regarding the claim recitation of "*scanning incoming content ... to*
9 *recognize the presence of potential computer exploits therewithin*", the examiner points
10 out that the prior art discloses such (e.g. Freund 29:34-30:9). Freund clearly teaches
11 the scanning of incoming content and the recognition of elements "known or suspected
12 to cause security or network problems". Thus, Freund discloses recognizing the
13 presence of potential computer exploits within incoming content.

14

15

16

Conclusion

17

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

20 A shortened statutory period for reply to this final action is set to expire THREE
21 MONTHS from the mailing date of this action. In the event a first reply is filed within
22 TWO MONTHS of the mailing date of this final action and the advisory action is not

Application/Control Number: 11/009,437
Art Unit: 2437

Page 10

1 mailed until after the end of the THREE-MONTH shortened statutory period, then the
2 shortened statutory period will expire on the date the advisory action is mailed, and any
3 extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of
4 the advisory action. In no event, however, will the statutory period for reply expire later
5 than SIX MONTHS from the mailing date of this final action.

6 Any inquiry concerning this communication or earlier communications from the
7 examiner should be directed to JEFFERY WILLIAMS whose telephone number is
8 (571)272-7965. The examiner can normally be reached on 8:30-5:00.

9 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
10 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone
11 number for the organization where this application or proceeding is assigned is 571-
12 273-8300.

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

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 11

1
2 /Jeffery Williams/
3 Examiner, Art Unit 2437
4
5 /Michael Pyzocha/
6 Primary Examiner, Art Unit 2437
7

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|------------------------------|---|-------------------------------|
| In Re Patent Application of: |) | |
| |) | Examiner: Jeffrey L. Williams |
| Moshe Rubin |) | |
| Moshe Matitya |) | Art Unit: 2437 |
| Artem Melnick |) | |
| Shlomo Touboul |) | |
| Alexander Yermakov |) | |
| Amit Shaked |) | |
| |) | |
| Application No: 11/009,437 |) | |
| |) | |
| Filed: December 9, 2004 |) | |
| |) | |
| For: METHOD AND SYSTEM FOR |) | |
| ADAPTIVE RULE-BASED |) | |
| CONTENT SCANNERS FOR |) | |
| DESKTOP COMPUTERS |) | |
| |) | |

FILED ELECTRONICALLY

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

AMENDMENT AND RESPONSE TO OFFICE ACTION
UNDER 37 C.F.R. §1.111

Sir:

In response to the Office Action dated September 18, 2009, applicants respectfully request that the above-identified application be amended as follows:

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

1. (currently amended) A security system for scanning content within a computer, comprising:

a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer;

a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs;

a rule-based content scanner that communicates with said database of parser and analyzer rules, operatively coupled with said network interface, for scanning incoming content received by said network interface to recognize the presence of potential computer exploits therewithin;

a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content scanner; and

a rule update manager that communicates with said database of parser and analyzer rules, for updating said database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

2. (previously presented) The security system of claim **1** wherein said database of parser and analyzer rules stores parser and analyzer rules in the form of pattern-matching engines.

3. (original) The security system of claim **2** wherein the pattern-matching engines are deterministic finite automata.

4. (original) The security system of claim **2** wherein the pattern-matching engines are non-deterministic finite automata.

5. (currently amended) The security system of claim **1** further comprising a content blocker, operatively coupled to said rule-based content scanner, for preventing incoming content having a computer exploit that was recognized by said rule-based content scanner from reaching its intended destination.

6. (currently amended) The system of claim **1** wherein the incoming content received from the Internet by said network interface is HTTP content.

7. (currently amended) The system of claim **1** wherein the incoming content received from the Internet by said network interface is HTTPS content.

8. (currently amended) The system of claim **1** wherein the incoming content received from the Internet by said network interface is FTP content

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

9. (currently amended) The system of claim **1** wherein the incoming content received from the Internet by said network interface is SMTP content

10. (currently amended) The system of claim **1** wherein the incoming content received from the Internet by said network interface is POP3 content

11. (original) The system of claim **1** wherein the destination Internet application is a web browser.

12. (original) The system of claim **1** wherein the destination Internet application is an e-mail client.

13. (currently amended) A method for scanning content within a computer, comprising:

receiving currently amended content from the Internet on its destination to an Internet application;

selectively diverting the received currently amended content from its intended destination;

scanning the selectively diverted currently amended content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs; and

updating the database of parser and analyzer rules periodically to incorporate new behavioral rules that are made available.

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

14. (previously presented) The method of claim **13** wherein said database of parser and analyzer rules stores parser and analyzer rules in the form of pattern-matching engines.

15. (original) The method of claim **14** wherein the pattern-matching engines are deterministic finite automata.

16. (original) The method of claim **14** wherein the pattern-matching engines are non-deterministic finite automata.

17. (currently amended) The method of claim **13** further comprising preventing incoming content having a computer exploit that was recognized by said scanning from reaching its intended destination.

18. (currently amended) The method of claim **13** wherein the incoming content received from the Internet by said network interface is HTTP content.

19. (currently amended) The method of claim **13** wherein the incoming content received from the Internet by said network interface is HTTPS content.

20. (currently amended) The method of claim **13** wherein the incoming content received from the Internet by said network interface is FTP content

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

21. (currently amended) The method of claim **13** wherein the incoming content received from the Internet by said network interface is SMTP content

22. (currently amended) The method of claim **13** wherein the incoming content received from the Internet by said network interface is POP3 content

23. (original) The method of claim **13** wherein the destination Internet application is a web browser.

24. (original) The method of claim **13** wherein the destination Internet application is an e-mail client.

25. (currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving incoming content from the Internet on its destination to an Internet application;

selectively diverting the received incoming content from its intended destination;

scanning the selectively diverted incoming content to recognize potential exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe exploits as logical combinations of patterns of program code constructs; and

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

updating the database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

REMARKS

Applicants have carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicants have amended claims **1, 5 – 10, 13, 17 – 22** and **25** to properly claim the present invention. No new matter has been added. Claims **1 - 25** are presented for examination.

On pages 2 – 4 of the Office Action, the Examiner has rejected claims **1, 2, 5, 6, 8 – 13, 17, 18** and **20 – 25** under 35 U.S.C. §102(e) as being anticipated by Freund, U.S. Patent No. 5,987,611 ("Freund").

On page 5 of the Office Action, the Examiner has rejected claims **3, 4, 7, 14 – 16** and **19** under 35 U.S.C. §103(a) as being unpatentable over Freund.

Response to Examiner's Arguments

On pages 6 and 7 of the Office Action, the Examiner has indicated that applicants' arguments are not persuasive because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentable distinguishes them from the references.

Applicants respectfully disagree. Applicants' arguments clearly pointed out that the specific claim language

"scanning the selectively diverted content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits ... wherein the

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs"

distinguishes the claims from the references.

Nevertheless, applicants further point out in detail hereinbelow how the language of the claims is distinguished over the references, and address each of the Examiner's arguments. Applicants wish to emphasize that the general spirit of Freund is fundamentally different than the spirit of the claimed invention. Freund concerns monitoring outbound access to the Internet, whereas the claimed invention concerns protection from inbound computer exploits. The title and headings of Freund make it clear that Freund is primarily concerned about unauthorized use of the Internet by company employees. Cf. the headings at 8:39 and col. 9:64, and the example at 9:37-53. Further, at 4:9-15, and at 13:2-18, Freund recites

"These access rules can include criteria such as total time a user can be connected to the Internet (e.g., per day, week, month, or the like), time a user can interactively use the Internet (e.g., per day, week, month, of the like), a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, ..."

At 5:31 - 6:27, Freund provides exemplary methodologies, including

"I. f) If the request for Internet access violates any of the rules transmitted to the particular client computer, denying the request for Internet access."

"II. c) If application is not allowed to access the Internet or not allowed to use the specific protocol then client monitor can stop the application from accessing the Internet and/or warn user."

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

"III. c) *If application has know[n] security problems, client monitor stops the application from accessing the Internet and/or warns the user.*"

"IV. b) *Client monitor determines whether the user interactively uses the Internet and restrict[s] the activity if required.*"

To further clarify this distinction, applicants have amended the claims to refer to the content as incoming content.

The rejections of the claims **1 - 25** on pages 2 - 5 of the Office Action will now be dealt with specifically.

As to amended independent claim **1** for a security system, applicant respectfully submits that the limitations in claim **1** of

"a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs", and

"a rule-based content scanner that communicates with said database of parser and analyzer rules, operatively coupled with said network interface, for scanning incoming content received by said network interface to recognize the presence of potential computer exploits therewithin"

are neither shown nor suggested in Freund.

In rejecting claim **1** the Examiner has cited Freund 21:33-40 as disclosing *"a rule update manager ... for updating ... parser and analyzer rules ..."* Applicants respectfully submit that Freund fails to disclose parser and analyzer rules for scanning inbound content. Instead, Freund describes a rules database for rules that define permitted outbound Internet activity by a client machine. Cf. Freund 4:8-19, 9:37-53 and 13:2-13.

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

Additionally, the Examiner has cited Freund FIG. 5:570 as disclosing a database of parser and analyzer rules corresponding to computer exploits. Applicants respectfully submit that Freund fails to disclose a database of parser and analyzer rules for scanning inbound content. Instead, database 570 stores rules which define permitted outbound activity for a client machine. Cf. Freund 21:26-31. Freund describes setting up rules by way of FIGS. 7A – K. At Freund 24:1-13 Freund recites

"For instance, an administrator can establish a rule based on a particular application, such as a rule pre[v]enting Internet access by a real audio player application (ra32.exe). Rules can also be established on the basis of including and/or excluding access to particular Internet sites. For instance, an administrator can establish a rule allowing users to only access a limited number of approved sites. On the other hand, the administrator can set a rule blocking user access to particular sites (e.g., pornographic sites). Rules can also be set which are time-based in nature. For instance, an administrator can establish a rule setting a time limit (e.g., 30 minutes) for how long a user can access the Internet each day ..."

As recited at Freund 24:36-39, Freund FIG. 7A:721 illustrates a rule that *"specifies that Web browsing is restricted to one hour per day for weekdays, from 9 a.m. to 6 p.m. The rule, which has a start day of Sep. 12, 1996, is currently configured to never expire."*

At Freund 27:9-16, Freund recites that *"a rule blocking a RealAudio application remains in force during working hours on weekdays – that is, at times when network traffic is already congested. At other times, however, the rule is not enforced. For the example shown in FIG. 7H, the*

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

rule has a start date of Mar. 31, 1997 and never expires; the rule is enforced weekdays and weekends from 8 a.m. to 5:30 p.m."

As such, it is clear that Freund does not disclose parser and analyzer rules for scanning inbound content.

Additionally, the Examiner has cited Freund, 23:44-55 as disclosing that "*parser and analyzer rules describe computer exploits as logical combination of patterns of program code constructs*".

Applicants respectfully submit that Freund fails to disclose such parser and analyzer rules. Instead, Freund discloses drivers for monitoring different types of outbound Internet access protocols made from a client machine. At 23:52-55, Freund recites "*Each driver is responsible for monitoring and filtering access for its particular type, including ensuring that any user activity which employs that access type conforms to any rules or conditions specified for the Internet monitor.*"

Additionally, the Examiner has cited Freund 29:54 – 30:9 as disclosing "*scanning content ... to recognize the presence of potential computer exploits therewithin*". Applicants wish to point out that computer exploits are defined within claim **1** as being portions of program code that are malicious. Freund discloses recognizing components of an HTML page, including JAVA™ applets, ActiveX controls, plug-ins, embedded scripts and references to other files or components. However, Freund does not analyze these components for the presence of computer exploits. Instead, Freund simply checks the rules database to see if a component is permissible. As such, Freund is unable to distinguish between a safe applet and a malicious applet. Freund simply allows or blocks all applets.

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

Because claims **2** – **12** depend from claim **1** and include additional features, applicants respectfully submit that claims **2** - **12** are not anticipated or rendered obvious by Freund.

Accordingly claims **1** – **12** are deemed to be allowable.

As to amended independent method claim **13** and amended independent claim **25** for a computer-readable storage medium, applicants respectfully submit that the limitation in claims **13** and **25** of

"scanning the selectively diverted incoming content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs"

is neither shown nor suggested in Freund.

The same remarks put forth above for the rejection of claim **1** apply to the rejections of claims **13** and **25**, since these claims were rejected for the same reasons on page 4 of the Office Action.

Because claims **14** – **24** depend from claim **13** and include additional features, applicants respectfully submit that claims **14** - **24** are not anticipated or rendered obvious by Freund.

Accordingly claims **13** – **25** are deemed to be allowable.

Support for Amended Claims in Original Specification

The term "content" has been amended in the claims to -- incoming content --. This limitation is supported in the original specification at least at pars. [0009], [0013], [0040], [00124], [00125] and [00140], and in FIGS. 9, 10 and 12 and the descriptions thereof.

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

CONCLUSION

The undersigned representative respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that the prosecution might be advanced by discussing the application with the undersigned representative, in person or over the telephone, we welcome the opportunity to do so. In addition, if any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account No. 504402.

Respectfully submitted,

Date: December 18, 2009
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4706
(202) 737-0500

By: /Eric L. Sophir, Reg. #48,499/
Eric L. Sophir
Registration No. 48,499



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. |
|---|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | FIN0001CON1CIP3CIP1 | 5071 |
| 74877 | 7590 | 09/18/2009 | EXAMINER | |
| King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006 | | | WILLIAMS, JEFFERY L | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2437 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 09/18/2009 | 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. 11/009,437 | Applicant(s) RUBIN ET AL. | |
| | Examiner JEFFERY WILLIAMS | Art Unit 2437 | |

-- 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 04 March 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) 1-25 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) 1-25 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 7/2/09.

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

5) Notice of Informal Patent Application

6) Other: _____.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 3

1 only if the international application designated the United States and was published under Article 21(2)
2 of such treaty in the English language.
3

4 **Claims 1, 2, 5, 6, 8 –12, 13, 17, 18, and 20 – 25 are rejected under 35**

5 **U.S.C. 102(e) as being anticipated by Freund, U.S. Patent, 5,987,611.**

6
7 Regarding claim 1, Freund discloses:

8 *a network interface, housed within a computer, for receiving content from the*
9 *Internet on its destination to an Internet application running on the computer (Freund,*
10 *fig. 2:220);*

11 *a database of parser and analyzer rules corresponding to computer exploits,*
12 *stored within the computer (Fruend, fig. 5:570), computer exploits being portions of*
13 *program code that are potentially malicious (Fruend, 29:54 – 30:9), wherein the parser*
14 *and analyzer rules describe computer exploits as logical combinations of patterns of*
15 *program code constructs (Fruend, 23:44-55; 28:14-16; 29:54 – 30:9); a rule-based*
16 *content scanner that communicates with said database of parser and analyzer rules,*
17 *operatively coupled with said network interface, for scanning content received by said*
18 *network interface to recognize the presence of potential computer exploits therewithin*
19 *(Fruend, 29:54-30:10); a network traffic probe, operatively coupled to said network*
20 *interface and to said rule-based content scanner, for selectively diverting content from*
21 *its intended destination to said rule-based content scanner (Freund, fig. 3a:311);*

22 *and a rule update manager that communicates with said database of parser and*
23 *analyzer rules, for updating said database of parser and analyzer rules periodically to*
24 *incorporate new parser and analyzer rules that are made available (Fruend, 21:33-40).*

Application/Control Number: 11/009,437
Art Unit: 2437

Page 4

1

2 Regarding claim 2, Freund discloses:

3 *wherein said database of parser and analyzer rules stores parser and analyzer*
4 *rules in the form of pattern-matching engines* (Freund, 29:54-30:10). Herein, Freund
5 discloses that the rules enable the driver or parser to operate according to a particular
6 manner.

7

8 Regarding claim 5, Freund discloses:

9 *a content blocker, operatively coupled to said rule-based content scanner, for*
10 *preventing content having a potential computer exploit that was recognized by said rule-*
11 *based content scanner from reaching its intended destination* (Freund, 15:22-16:7).

12

13 Regarding claims 6, 8 – 10, Freund discloses:

14 *wherein the content received from the Internet by said network interface is HTTP,*
15 *FTP, SMTP, POP3 content* (Freund, 23:44-55).

16

17 Regarding claims 11 and 12, Freund discloses:

18 *wherein the destination Internet application is a web browser; wherein the*
19 *destination Internet application is an e-mail client* (12:18-42).

20

21 Regarding claims 13, 17, 18, 20 – 25, they are rejected, at least, for the same
22 reasons as claims 1, 5, 6, 8 – 12.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 5

1

2

Claim Rejections - 35 USC § 103

3

4

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

5

obviousness rejections set forth in this Office action:

6

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

7

8

9

10

11

12

Claims 7 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable

13

over Freund, U.S. Patent, 5,987,611.

14

15

Regarding claims 7 and 19, Freund discloses that the system is flexible so as to

16

support a plurality of protocols (Freund, 12:18-42). While Freund discloses supporting

17

existing protocols such as HTTP, Freund does not appear to explicitly state that the

18

system may support secure HTTP. However, it would have been obvious to one of

19

ordinary skill in the art to employ support for the secure HTTP because one of ordinary

20

skill in the art would have been motivated by increased flexibility of the system.

21

22

Regarding claims 3, 4, and 14 – 16, Freund discloses parsing means for pattern

23

matching, but does not appear to disclose DFA or NDFA. However, the examiner notes

24

that it was well known in the art for DFA and NDFA to be used as engines for pattern

25

matching (e.g. see admission by the applicant, Applicant's specification, par. 73).

26

Application/Control Number: 11/009,437
Art Unit: 2437

Page 6

1

2

Response to Arguments

3

4

Applicant's arguments filed 3/4/09 have been fully considered but they are not

5

persuasive.

6

7

Applicant argues or asserts essentially that:

8

... the limitations in claim **1** of

9

"a database of parser and analyzer rules corresponding to computer

10

exploits, stored within the computer, computer exploits being portions of program code

11

that are potentially malicious, wherein the parser and analyzer rules describe computer

12

exploits as logical combinations of patterns of program code constructs", and

13

"a rule-based content scanner that communicates with said database of

14

parser and analyzer rules, operatively coupled with said network interface, for scanning

15

content received by said network interface to recognize the presence of computer

16

exploits therewithin"

17

are neither shown nor suggested in Freund. Therefore, Freund fails to disclose each

18

and every element of claim 1 as required by 35 U.S.C. § 102(e). **(Remarks, pg. 10)**

19

... the limitation in claims **13** and **25** of *"scanning the selectively diverted content*

20

to recognize potential exploits therewithin, based on a database of parser and analyzer

21

rules corresponding to computer exploits, computer exploits being portions of program

Application/Control Number: 11/009,437
Art Unit: 2437

Page 7

1 *code that are potentially malicious, wherein the parser and analyzer rules describe*
2 *computer exploits as logical combinations of patterns of program code constructs"*
3 is neither shown nor suggested in Freund. Therefore, Freund fails to disclose each and
4 every element of claims 13 and 25 as required by 35 U.S.C. § 102(e). **(Remarks,**
5 **pg. 11)**

6

7 *Examiner respectfully responds::*

8 The examiner respectfully notes that the applicant's argument comprises only an
9 allegation that the claim recitations are novel in view of prior art and fail to comprise any
10 evidence, line of argument, or rationale for support.

11 Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount
12 to a general allegation that the claims define a patentable invention without specifically
13 pointing out how the language of the claims patentably distinguishes them from the
14 references.

15

16

Conclusion

17

18 The prior art made of record and not relied upon is considered pertinent to
19 applicant's disclosure:

20

See Notice of References Cited.

21

Application/Control Number: 11/009,437
Art Unit: 2437

Page 8

1 A shortened statutory period for reply is set to expire **3** months (not less than 90
2 days) from the mailing date of this communication.

3 Any inquiry concerning this communication or earlier communications from the
4 examiner should be directed to Jeffery Williams whose telephone number is (571) 272-
5 7965. The examiner can normally be reached on 8:30-5:00.

6 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
7 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone
8 number for the organization where this application or proceeding is assigned is (703)
9 872-9306.

10 Information regarding the status of an application may be obtained from the
11 Patent Application Information Retrieval (PAIR) system. Status information for
12 published applications may be obtained from either Private PAIR or Public PAIR.
13 Status information for unpublished applications is available through Private PAIR only.
14 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
15 you have questions on access to the Private PAIR system, contact the Electronic
16 Business Center (EBC) at 866-217-9197 (toll-free).

17

18
19 /Jeffery Williams/
20 Examiner, Art Unit 2437

21
22 /Emmanuel L. Moise/
23 Supervisory Patent Examiner, Art Unit 2437
24

Attorney's Docket No.: FIN0001-CON1-CIP3-CIP1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|------------------------------|---|-------------------------------|
| In Re Patent Application of: |) | |
| |) | Examiner: Jeffery L. Williams |
| Moshe Rubin |) | |
| Moshe Matitya |) | Art Unit: 2437 |
| Artem Melnick |) | |
| Shlomo Touboul |) | |
| Alexander Yermakov |) | |
| Amit Shaked |) | |
| |) | |
| Application No: 11/009,437 |) | |
| |) | |
| Filed: December 9, 2004 |) | |
| |) | |
| For: METHOD AND SYSTEM FOR |) | |
| ADAPTIVE RULE-BASED |) | |
| CONTENT SCANNERS FOR |) | |
| DESKTOP COMPUTERS |) | |
| _____ |) | |

FILED ELECTRONICALLY

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

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION

UNDER 37 C.F.R. §1.116

Sir:

In response to the Final Office Action dated January 13, 2009, applicants respectfully request that the above-identified application be amended as follows:

IN THE SPECIFICATION:

Please further amend page 18, 1st full paragraph of the original specification as follows:

[0053] In order to accelerate the scanning process, pre-scanner 150 acts as a first-pass filter, to filter content that can be quickly recognized as innocuous. Content that is screened by pre-scanner 150 as being potentially malicious is passed along to ARB scanner 130 for further diagnosis. Content that is screened by pre-scanner 150 as being innocuous bypasses ARB scanner 130. It is expected that pre-scanner 150 filters 90% of incoming content, and that only 10% of the content requires extensive scanning by ARB scanner 130. As such, the combined effect of ARB scanner 130 and pre-scanner 150 provides an average scanning throughout of approximately 9 mega-bits per second.

Please amend page 40, 1st full paragraph of the original specification as follows:

[00141] In accordance with a preferred embodiment of the present invention, over-blocking of content with conditionally malicious code is mitigated by integrating ARB scanner 1210 with sandbox scanner 1230. Sandbox scanner 1230 analyzes content by executing the content within a protected environment, so that the content does not have access to critical system data including inter alia operating system data, file system data and network communication data. The analysis performed by sandbox scanner 1230 is specific to one set of values of operational data; namely, the values at the time the content is executed.

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

1. (currently amended) A security system for scanning content within a computer, comprising:

a network interface, housed within a computer, for receiving content from the Internet on its destination to an Internet application running on the computer;

a database of ~~behavioral~~ parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are ~~potentially~~ malicious, wherein the ~~behavioral~~ parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs;

a rule-based content scanner that communicates with said database of ~~behavioral~~ parser and analyzer rules, operatively coupled with said network interface, for scanning content received by said network interface to recognize the presence of potential computer exploits therewithin;

a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting content from its intended destination to said rule-based content scanner; and

a rule update manager that communicates with said database of ~~behavioral~~ parser and analyzer rules, for updating said database of ~~behavioral~~ parser and analyzer rules periodically to

incorporate new ~~behavioral~~ parser and analyzer rules that are made available.

2. (currently amended) The security system of claim **1** wherein said database of ~~behavioral~~ parser and analyzer rules stores ~~behavioral~~ parser and analyzer rules in the form of pattern-matching engines.

3. (original) The security system of claim **2** wherein the pattern-matching engines are deterministic finite automata.

4. (original) The security system of claim **2** wherein the pattern-matching engines are non-deterministic finite automata.

5. (previously presented) The security system of claim **1** further comprising a content blocker, operatively coupled to said rule-based content scanner, for preventing content having a computer exploit that was recognized by said rule-based content scanner from reaching its intended destination.

6. (original) The system of claim **1** wherein the content received from the Internet by said network interface is HTTP content.

7. (original) The system of claim **1** wherein the content received from the Internet by said network interface is HTTPS content.

8. (original) The system of claim **1** wherein the content received from the Internet by said network interface is FTP content

9. (original) The system of claim **1** wherein the content received from the Internet by said network interface is SMTP content

10. (original) The system of claim **1** wherein the content received from the Internet by said network interface is POP3 content

11. (original) The system of claim **1** wherein the destination Internet application is a web browser.

12. (original) The system of claim **1** wherein the destination Internet application is an e-mail client.

13. (currently amended) A method for scanning content within a computer, comprising:

receiving content from the Internet on its destination to an Internet application;

selectively diverting the received content from its intended destination;

scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of ~~behavioral~~ parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are ~~potentially~~ malicious, wherein the ~~behavioral~~ parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs; and

updating the database of ~~behavioral~~ parser and analyzer rules periodically to incorporate new behavioral rules that are made available.

14. (currently amended) The method of claim **13** wherein said database of ~~behavioral~~ parser and analyzer rules stores ~~behavioral~~ parser and analyzer rules in the form of pattern-matching engines.

15. (original) The method of claim **14** wherein the pattern-matching engines are deterministic finite automata.

16. (original) The method of claim **14** wherein the pattern-matching engines are non-deterministic finite automata.

17. (previously presented) The method of claim **13** further comprising preventing content having a computer exploit that was recognized by said scanning from reaching its intended destination.

18. (original) The method of claim **13** wherein the content received from the Internet by said network interface is HTTP content.

19. (original) The method of claim **13** wherein the content received from the Internet by said network interface is HTTPS content.

20. (original) The method of claim **13** wherein the content received from the Internet by said network interface is FTP content

21. (original) The method of claim **13** wherein the content received from the Internet by said network interface is SMTP content

22. (original) The method of claim **13** wherein the content received from the Internet by said network interface is POP3 content

23. (original) The method of claim **13** wherein the destination Internet application is a web browser.

24. (original) The method of claim **13** wherein the destination Internet application is an e-mail client.

25. (currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving content from the Internet on its destination to an Internet application;

selectively diverting the received content from its intended destination;

scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of ~~behavioral~~ parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are ~~potentially~~ malicious, wherein the ~~behavioral~~ parser and analyzer rules describe exploits as logical combinations of patterns of program code constructs; and

updating the database of ~~behavioral~~ parser and analyzer rules periodically to incorporate new ~~behavioral~~ parser and analyzer rules that are made available.

REMARKS

Applicants have carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicants have amended claims **1, 2, 13, 14** and **25** to properly claim the present invention. No new matter has been added. Claims **1 - 25** are presented for examination.

On page 2 of the Office Action, the Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

On pages 2 and 3 of the Office Action, the Examiner has rejected claims **1 - 25** under 35 U.S.C. §112 first paragraph as failing to comply with the written description requirement.

Applicants respectfully submit that the section entitled "Support for New and Amended Claims in Original Specification" in applicants' previous response, points out where the previously amended claims are supported. The following table summarizes the support.

| TABLE: Support provided for previously amended claims in applicant's response filed on November 4, 2008 | |
|--|--|
| Location in original specification | Support |
| Par. [0011] | <i>"Rule files for a language describe character encodings, sequences of characters that form lexical constructs of the language, referred to as <u>tokens</u>, patterns of tokens that form syntactical constructs of program code, referred to as <u>parsing rules</u>, and patterns of tokens that correspond to potential exploits, referred to as <u>analyzer rules</u>."</i> |
| Par. [0012] | <i>"This description language enable an engineer to describe exploits as logical combinations of patterns of tokens."</i> |

| | |
|---------------------------|---|
| Par. [0042] | <i>"Portions of code that are malicious are referred to as exploits."</i> |
| Par. [0044] | <i>"... a behavioral approach that analyses content based on its behavior instead of its binary structure."</i> |
| Par. [0055] | <i>"An ARB scanner system ... is customized for a specific language through use of a set of language-specific rules."</i> |
| Par. [0056] | <i>"Moreover ... security violations, referred to as exploits, are described using a generic syntax, which is also language-independent."</i> |
| Par. [0057] | <i>"... a set of rules that serve to train the content scanner how to interpret the language ... the ability to describe exploits using a generic syntax ..."</i> |
| Par. [0066] | <i>"Preferably, the rule file describes text characters used within the content language, and the composition of constructs of the content language ..."</i> |
| Par. [0082] | <i>"An analyzer rule specifies a general syntax pattern ... that indicates a potential exploit ... rules are provided to analyzer 230 for each known exploit"</i> |
| Pars. [0097] – [00102] | Analyzer rule for the exploit indicated in Pars. [0042] and [0043] |
| Par. [00103] | <i>"... exploits are generally described in terms of composite pattern matches, involving logical combinations of more than one pattern."</i> |
| Pars. [00111] and [00112] | <i>"... the parser calls an analyzer ... to determine if a potential exploit is present within the current parse tree ... the parser checks whether or not the analyzer found a match for an analyzer rule ..."</i> |
| Par. [00113] | <i>"Preferably, the rule files are generated by one or more people who are familiar with the content languages."</i> |
| Par. [00122] | <i>"... the method may stop as soon as a first analyzer rule is matched ... to determine that the scanned content contains a potential exploit."</i> |
| Par. [00125] | <i>"... a database 940 of coded exploit rules ... which perform pattern matches appropriate to exploits ..."</i> |
| Par. [00126] | <i>"In order to keep exploit rule database 940 current, desktop computer 800 preferably includes a rules update manager 960, which periodically receives modified rules and new rules over the Internet, and updates database 940 accordingly."</i> |
| Par. [00127] | <i>"... a rule server that updates rule databases for the desktop computer ..."</i> |
| Par. [00128] | <i>"... enables rule server 1010 to propagate the most up-to-date rules to a plurality of desktop computer, and enables rule engineers to continually build up a database of exploit rules."</i> |
| FIG. 9 | Exploit rules database 940; rules update manager 960 |
| FIG. 10 | Rules update server 1010 |
| APPENDIX A | Rule file for JavaScript |

Therefore, it is respectfully requested that the rejection under 35 U.S.C. §112 be withdrawn.

On pages 3 – 5 of the Office Action, the Examiner has rejected claims **1, 2, 5, 6, 8 – 13, 17, 18** and **20 – 25** under 35 U.S.C. §102(e) as being anticipated by Freund, U.S. Patent No. 5,987,611 (“Freund”).

On page 6 of the Office Action, the Examiner has rejected claims **3, 4, 7, 14 – 16** and **19** under 35 U.S.C. §103(a) as being unpatentable over Freund.

Response to Examiner’s Arguments

In the Examiner’s Response to Arguments on pages 7 – 9 of the Office Action, the Examiner has indicated that the features upon which applicants rely are not recited in the claims. Applicants have accordingly amended independent claims **1, 13** and **25** to include the limitations of parser rules and analyzer rules.

As to amended independent claim **1** for a security system, applicant respectfully submits that the limitations in claim **1** of

“a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are potentially malicious, wherein the parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs”, and

“a rule-based content scanner that communicates with said database of parser and analyzer rules, operatively coupled with said network interface, for scanning content received by said network interface to recognize the presence of computer exploits therewithin”

are neither shown nor suggested in Freund. Therefore, Freund fails to disclose each and every element of claim **1** as required by 35 U.S.C. § 102(e).

Because claims **2** – **12** depend from claim **1** and include additional features, applicants respectfully submit that claims **2** - **12** are not anticipated or rendered obvious by Freund.

Accordingly claims **1** – **12** are deemed to be allowable.

As to amended independent method claim **13** and amended independent claim **25** for a computer-readable storage medium, applicants respectfully submit that the limitation in claims **13** and **25** of

"scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are potentially malicious, wherein the parser and analyzer rules describe computer exploits as logical combinations of patterns of program code constructs"

is neither shown nor suggested in Freund. Therefore, Freund fails to disclose each and every element of claims **13** and **25** as required by 35 U.S.C. § 102(e).

Because claims **14** – **24** depend from claim **13** and include additional features, applicants respectfully submit that claims **14** - **24** are not anticipated or rendered obvious by Freund.

Accordingly claims **13** – **25** are deemed to be allowable.

Therefore, it is respectfully requested that the rejection of claims **1** - **25** under 35 U.S.C. §§ 102(e) and 103(a) be withdrawn.

Support for New and Amended Claims in Original Specification

Amended independent claims **1**, **13** and **25** include the limitations of parser and analyzer rules that describe computer exploits as logical combinations of patterns of program code constructs. Support for these limitations in the original specification is provided in the table

hereinabove. In addition, specific examples of parser and analyzer rules for JavaScript are provided in Appendix A of the original specification, at pages 47 – 52.

CONCLUSION

The undersigned representative respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that the prosecution might be advanced by discussing the application with the undersigned representative, in person or over the telephone, we welcome the opportunity to do so. In addition, if any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account 50-4402.

Respectfully submitted,

Date: February 17, 2009 By: /Eric L. Sophir Reg. No. 48,499/
KING & SPALDING LLP Eric L. Sophir
1700 Pennsylvania Ave., NW Registration No. 48,499
Suite 200
Washington, DC 20006
(202) 737-0500



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. |
|---|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | FIN0001CON1CIP3CIP1 | 5071 |
| 74877 | 7590 | 01/13/2009 | EXAMINER | |
| King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006 | | | WILLIAMS, JEFFERY L | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2437 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 01/13/2009 | 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.

Application/Control Number: 11/009,437
Art Unit: 2437

Page 3

1 **Claims 1 – 25 are rejected under 35 U.S.C. 112, first paragraph, as failing to**
2 **comply with the written description requirement.** The claim(s) contains subject
3 matter which was not described in the specification in such a way as to reasonably
4 convey to one skilled in the relevant art that the inventor(s), at the time the application
5 was filed, had possession of the claimed invention. Applicant has not pointed out where
6 the new (or amended) claim is supported, nor does there appear to be a written
7 description of the claim limitations in the application as filed (see above objection to the
8 specification). For example, the applicant's specification lacks disclosure of the idea of
9 "behavioral rules". Furthermore, while the applicant's specification discloses finding
10 "*potential exploits*", there is no disclosure of "computer exploits being portions of
11 program code that are potentially malicious". Additionally, while the applicant's
12 specification discloses rules that describe constructs *corresponding* to exploits, the
13 specification fails to disclose "behavioral rules describe computer exploits as logical
14 combinations of patterns of program code constructs".

15
16

17 ***Claim Rejections - 35 USC § 102***

18

19 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that
20 form the basis for the rejections under this section made in this Office action:

21

A person shall be entitled to a patent unless –

22
23
24
25
26

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

Application/Control Number: 11/009,437
Art Unit: 2437

Page 4

1 only if the international application designated the United States and was published under Article 21(2)
2 of such treaty in the English language.
3

4 **Claims 1, 2, 5, 6, 8 –12, 13, 17, 18, and 20 – 25 are rejected under 35**

5 **U.S.C. 102(e) as being anticipated by Freund, U.S. Patent, 5,987,611.**

6
7 Regarding claim 1, Freund discloses:

8 *a network interface, housed within a computer, for receiving content from the*
9 *Internet on its destination to an Internet application running on the computer (Freund,*
10 *fig. 2:220);*

11 *a database of behavioral rules corresponding to computer exploits, stored within*
12 *the computer (Fruend, fig. 5:570), computer exploits being portions of program code*
13 *that are potentially malicious (Fruend, 29:54 – 30:9), wherein the behavioral rules*
14 *describe computer exploits as logical combinations of patterns of program code*
15 *constructs (Fruend, 23:44-55; 28:14-16; 29:54 – 30:9); a rule-based content scanner*
16 *that communicates with said database of behavioral rules, operatively coupled with said*
17 *network interface, for scanning content received by said network interface to recognize*
18 *the presence of computer exploits therewithin (Fruend, 29:54-30:10); a network traffic*
19 *probe, operatively coupled to said network interface and to said rule-based content*
20 *scanner, for selectively diverting content from its intended destination to said rule-based*
21 *content scanner (Freund, fig. 3a:311);*

22 *and a rule update manager that communicates with said database of behavioral*
23 *rules, for updating said database of behavioral rules periodically to incorporate new*
24 *behavioral rules that are made available (Freund, 21:33-40).*

Application/Control Number: 11/009,437
Art Unit: 2437

Page 5

1

2 Regarding claim 2, Freund discloses:

3 *wherein said database of behavioral rules stores behavioral rules in the form of*
4 *pattern-matching engines* (Freund, 29:54-30:10). Herein, Freund discloses that the
5 rules enable the driver or parser to operate according to a particular manner.

6

7 Regarding claim 5, Freund discloses:

8 *a content blocker, operatively coupled to said rule-based content scanner, for*
9 *preventing content having a potential computer exploit that was recognized by said rule-*
10 *based content scanner from reaching its intended destination* (Freund, 15:22-16:7).

11

12 Regarding claims 6, 8 – 10, Freund discloses:

13 *wherein the content received from the Internet by said network interface is HTTP,*
14 *FTP, SMTP, POP3 content* (Freund, 23:44-55).

15

16 Regarding claims 11 and 12, Freund discloses:

17 *wherein the destination Internet application is a web browser; wherein the*
18 *destination Internet application is an e-mail client* (12:18-42).

19

20 Regarding claims 13, 17, 18, 20 – 25, they are rejected, at least, for the same
21 reasons as claims 1, 5, 6, 8 – 12.

22

Application/Control Number: 11/009,437
Art Unit: 2437

Page 6

1 **Claim Rejections - 35 USC § 103**

2

3

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

4

obviousness rejections set forth in this Office action:

5

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

6

7

8

9

10

11

Claims 7 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable

12

over Freund, U.S. Patent, 5,987,611.

13

14

Regarding claims 7 and 19, Freund discloses that the system is flexible so as to

15

support a plurality of protocols (Freund, 12:18-42). While Freund discloses supporting

16

existing protocols such as HTTP, Freund does not appear to explicitly state that the

17

system may support secure HTTP. However, it would have been obvious to one of

18

ordinary skill in the art to employ support for the secure HTTP because one of ordinary

19

skill in the art would have been motivated by increased flexibility of the system.

20

21

Regarding claims 3, 4, and 14 – 16, Freund discloses parsing means for pattern

22

matching, but does not appear to disclose DFA or NDFA. However, the examiner notes

23

that it was well known in the art for DFA and NDFA to be used as engines for pattern

24

matching (e.g. see admission by the applicant, Applicant's specification, par. 73).

25

26

Application/Control Number: 11/009,437
Art Unit: 2437

Page 7

1

Response to Arguments

2

3 Applicant's arguments filed 11/12/08 have been fully considered but they are not
4 persuasive.

5

6 Applicant argues or asserts essentially that:

7

8 (i) *In distinction to Freund, the rules used in the subject claimed invention are parser*
9 *rules and analyzer rules, which describe program source code exploits in terms of*
10 *logical combinations of constructs of a specific programming language (original*
11 *specification/pars. 11, 55, 56, 66, 67, 81, 82 and 103). The rules used in Freund are*
12 *Internet access rules, which limit a user's use of the Internet. (Remarks, pg. 19)*

13

14 In response to applicant's argument that the references fail to show certain
15 features of applicant's invention, it is noted that the features upon which applicant relies
16 (i.e., parser rules and analyzer rules) are not recited in the rejected claim(s). Although
17 the claims are interpreted in light of the specification, limitations from the specification
18 are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057
19 (Fed. Cir. 1993).

20

21 (ii) *In order to further clarify this distinction, applicants have amended the term*
22 *"rules" to behavioral rules, to distinguish them from the access rules of Freund.*

Application/Control Number: 11/009,437
Art Unit: 2437

Page 8

1 *Applicants have further added the limitations that exploits are portions of program code*
2 *that are potentially malicious, and that the behavioral rules describe exploits as logical*
3 *combinations of patterns of program code constructs. (Remarks, pg. 19)*
4

5 Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount
6 to a general allegation that the claims define a patentable invention without specifically
7 pointing out how the language of the claims patentably distinguishes them from the
8 references.

9

10 (iii) *However, Freund's access rules do not describe how to recognize exploits within*
11 *such components; i.e., within the Java program code, the ActiveX program code, the*
12 *plug-in program code, the JavaScript program code and the VBScript program code that*
13 *the user/workstation is trying to access. Instead, Freund simply denies access*
14 *altogether. (Remarks, pg. 21)*
15

16 In response to applicant's argument that the references fail to show certain
17 features of applicant's invention, it is noted that the features upon which applicant relies
18 (i.e., *describe how to recognize exploits within such components; i.e., within the Java*
19 *program code, the ActiveX program code, the plug-in program code, the JavaScript*
20 *program code and the VBScript program code that the user/workstation is trying to*
21 *access.*) are not recited in the rejected claim(s). Although the claims are interpreted in

Application/Control Number: 11/009,437
Art Unit: 2437

Page 9

1 light of the specification, limitations from the specification are not read into the claims.
2 See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

3

4

Conclusion

5

6 The prior art made of record and not relied upon is considered pertinent to
7 applicant's disclosure:

8

See Notice of References Cited.

9

10 Applicant's amendment necessitated the new ground(s) of rejection presented in
11 this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP
12 § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37
13 CFR 1.136(a).

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

Application/Control Number: 11/009,437
Art Unit: 2437

Page 10

1 Any inquiry concerning this communication or earlier communications from the
2 examiner should be directed to Jeffery Williams whose telephone number is (571) 272-
3 7965. The examiner can normally be reached on 8:30-5:00.

4 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
5 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone
6 number for the organization where this application or proceeding is assigned is (703)
7 872-9306.

8 Information regarding the status of an application may be obtained from the
9 Patent Application Information Retrieval (PAIR) system. Status information for
10 published applications may be obtained from either Private PAIR or Public PAIR.
11 Status information for unpublished applications is available through Private PAIR only.
12 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
13 you have questions on access to the Private PAIR system, contact the Electronic
14 Business Center (EBC) at 866-217-9197 (toll-free).

15

16

17 J. Williams
18 AU 2437

19

20 /Emmanuel L. Moise/
21 Supervisory Patent Examiner, Art Unit 2437

22

23

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|------------------------------|---|-------------------------------|
| In Re Patent Application of: |) | |
| |) | Examiner: Jeffrey L. Williams |
| Moshe Rubin |) | |
| Moshe Matitya |) | Art Unit: 2137 |
| Artem Melnick |) | |
| Shlomo Touboul |) | |
| Alexander Yermakov |) | |
| Amit Shaked |) | |
| |) | |
| Application No: 11/009,437 |) | |
| |) | |
| Filed: December 9, 2004 |) | |
| |) | |
| For: METHOD AND SYSTEM FOR |) | |
| ADAPTIVE RULE-BASED |) | |
| CONTENT SCANNERS FOR |) | |
| DESKTOP COMPUTERS |) | |
| |) | |

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

AMENDMENT AND RESPONSE TO OFFICE ACTION
UNDER 37 C.F.R. §1.111

Sir:

In response to the Office Action dated September 5, 2008, applicants respectfully request that the above-identified application be amended as follows:

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

IN THE SPECIFICATION:

Please amend page 1, 1st full paragraph of the original specification as follows:

[00128] This application is a continuation-in-part of assignee's pending application U.S. Serial No. 10/930,884, filed on August 30, 2004, entitled "Method and System for Adaptive Rule-Based Content Scanners," which is a continuation-in-part of assignee's pending application U.S. Serial No. 09/539,667, filed on March 30, 2000, now U.S. Patent No. 6,804,780, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables," which is a continuation of assignee's patent application U.S. Serial No. U.S. Ser. No. 08/964,388, filed on 6 November 1997, now U.S. Patent No. 6,092,194, also entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables."

Please amend page 3, 3rd full paragraph of the original specification as follows:

[0011] The content scanners of the present invention are referred to as adaptive rule-based (ARB) scanners. An ARB scanner is able to adapt itself dynamically to scan a specific type of content, such as inter alia JavaScript, VBScript, URI, URL and [[HTTP]] HTML. ARB scanners differ from prior art scanners that are hard-coded for one particular type of content. In distinction, ARB scanners are data-driven, and can be enabled to scan any specific type of content by providing appropriate rule files, without the need to modify source code. Rule files are text files that describe lexical characteristics of a particular language. Rule files for a language describe character encodings, sequences of characters that form

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

lexical constructs of the language, referred to as tokens, patterns of tokens that form syntactical constructs of program code, referred to as parsing rules, and patterns of tokens that correspond to potential exploits, referred to as analyzer rules. Rules files thus serve as adaptors, to adapt an ARB content scanner to a specific type of content.

Please amend page 12, 11th full paragraph of the original specification as follows:

[0034] FIG. 9 is a simplified block diagram of a desktop computer implementation of an ARB content scanner, in accordance with a preferred embodiment of the present invention; [[and]]

Please amend page 16, 2nd full paragraph of the original specification as follows:

[0045] In accordance with a preferred embodiment of the present invention, network gateway 110 includes a content scanner 130, whose purpose is to scan mobile code and identify potential exploits. Content scanner 130 receives as input content containing mobile code in the form of byte source, and generates a security profile for the content. The security profile indicates whether or not potential exploits have been discovered within the content, and, if so, provides a diagnostic list of one or more potential exploits and their respective locations within the content.

Please amend page 16, 3rd full paragraph of the original specification as follows:

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

[0046] Preferably, the corporate intranet uses a security policy to decide whether or not to block incoming content based on the content's security profile. For example, a security policy may block content that may be severely malicious, say, content that accesses an operating system or a file system, and may permit content that is less malicious, such as content that can consume a user's computer screen as in the example above. The diagnostics within a content security profile are compared ~~within~~ with the intranet security policy, and a decision is made to allow or block the content. When content is blocked, one or more alternative actions can be taken, such as replacing suspicious portions of the content with innocuous code and allowing the modified content, and sending a notification to an intranet administrator.

Please amend page 17, 1st full paragraph of the original specification as follows:

[0047] Scanned content and their corresponding security profiles are preferably stored within a content cache 140. Preferably, network gateway 110 checks if incoming content is already resident in cache 140, and, if so, bypasses content scanner 130. Use of cache 140 saves content scanner 130 the task of re-scanning the same content.

Please amend page 17, 3rd full paragraph of the original specification as follows:

[0049] Consider, for example, a complicated JavaScript file that is scanned and determined to contain a known exploit therewithin. An MD5 hash value of the entire JavaScript file can be stored in cache, together ~~within~~ with a

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

security profile indicating that the JavaScript file contains the known exploit. If the same JavaScript file arrives again, its hash value is computed and found to already reside in cache. Thus, it can immediately be determined that the JavaScript file contains the known exploit, without re-scanning the file.

Please amend page 18, 1st full paragraph of the original specification as follows:

[0053] In order to accelerate the scanning process, pre-scanner 150 acts as a first-pass filter, to filter content that can be quickly recognized as innocuous. Content that is screened by pre-scanner 150 as being potentially malicious is passed along to ARB scanner 130 for further diagnosis. Content that is screened by pre-scanner 150 as being innocuous bypasses ARB scanner 130. It is expected that pre-scanner filters 90% of incoming content, and that only 10% of the content ~~required~~ requires extensive scanning by ARB scanner 130. As such, the combined effect of ARB scanner 130 and pre-scanner 150 provides an average scanning throughout of approximately 9 mega-bits per second.

Please amend page 18, 2nd full paragraph of the original specification as follows:

[0054] Use of security profiles, security policies and caching is described in applicant's U.S. Patent No. 6,092,194 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, in applicant's U.S. Patent ~~Application~~ ~~Serial~~ No. ~~09/539,667~~ 6,804,780 entitled SYSTEM AND METHOD FOR PROTECTING A

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES ~~and filed on 30 March 2000~~, and in applicant's U.S. Patent Application Serial No. ~~10/838,889~~ 7,418,731 entitled METHOD AND SYSTEM FOR CACHING AT SECURE GATEWAYS. ~~GATEWAYS and filed on 3 May 2004~~

Please amend page 20, 2nd full paragraph of the original specification as follows:

[0061] Reference is now made to FIG. 3, which is an illustration of a simple finite state machine for detecting tokens "a" and "ab", used in accordance with a preferred embodiment of the present invention. Shown in FIG. 3 are five states, 1 – 5, with labeled and directed transitions therebetween. As tokenizer reads successive characters, a transition is made from a current state to a next state accordingly. [[210]] State 1 is an entry state, where tokenizer 210 begins. State 4 is a generic state for punctuation. Specifically, whenever a punctuation character is encountered, a transition is made from the current state to state 4. The "a" token is identified whenever a transition is made from state 3 to state 4. Similarly, the "ab" token is identified whenever a transition is made from state 5 to state 4. A generic token, other than "a" and "ab" is identified whenever a transition is made from state 2 to state 4. A punctuation token is identified whenever a transition is made out of state 4.

Please amend page 22, 2nd full paragraph of the original specification as follows:

[0068] Preferably, the parse tree generated by parser 220 is dynamically built using a shift-and-reduce algorithm. Successive tokens

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

provided to parser 220 by tokenizer 210 are positioned as siblings. When parser 220 discovers that a parsing rule identifies [[of]] a group of siblings as a single pattern, the siblings are reduced to a single parent node by positioning a new parent node, which represents the pattern, in their place, and moving them down one generation under the new parent note.

Please amend page 24, 2nd full paragraph of the original specification as follows:

[0077] Reference is now made to FIG. 4B, which is a DFA corresponding to the NFA of FIG. 4A. In ~~contrast~~ contrast to the NFA of FIG. 4A, there are no nodes in the DFA labeled "epsilon," and each node in the DFA has at most one permissible outgoing edge, for any given token. As such, there is no need for the DFA to ever back track. All of the nodes with double circles around them are finishing nodes. If the sequence of tokens 1001 1002 1003 1004 1001 is input, then the DFA processes the tokens 1001 1002 1003 1004 and proceeds through the path with successive nodes 1, 2, 3, 8 and 9. There is no outgoing edge at node 9 corresponding to the next token 1001 in the input sequence. As such, the DFA terminates successfully with the pattern 1001 1002 1003 1004.

Please amend page 33, 2nd full paragraph of the original specification as follows:

[00110] At step 620 the parser checks whether or not a pattern is matched, based on parser rules within a rule file for the specific content language. If not, then control returns to step 600, for processing the next token. If a match with a parser rule is discovered at step 620, then at step

Attorney's Docket No.: FIN0001C1CIP3CIP1*PATENT*

630 the parser checks whether or not the matched parser rule has a "nonode" attribute. If so, then control returns to step 600. If the matched parser rule does not have a "nonode" attribute, then at step 640 the parser performs the matched parser rule's action. Such action can include inter alia creation of a new node, naming the new node according to the matched parser rule, and placing the matching [[node]] nodes underneath the new node, as indicated at step 640. Thus it may be appreciated that nodes within the parse tree have names that correspond either to names of tokens, or names of parser rules.

Please amend page 33, 3rd full paragraph of the original specification as follows:

[00111] At step 650 the parser checks whether or not the matched parser [[rules]] rule has a "noanalyze" attribute. If so, then control returns to step 620. If the matched parser [[rules]] rule does not have a "noanalyze" attribute, then at step 660 the parser calls an analyzer, such as analyzer 230, to determine if a potential exploit is present within the current parse tree. It may thus be appreciated that the analyzer is called repeatedly, while the parse tree is being dynamically built up.

Please amend page 34, 4th full paragraph of the original specification as follows:

[00117] Reference is now made to FIG. 8, which illustrates a representative hierarchy of objects created by builder module 720, in accordance with a preferred embodiment of the present invention. Shown in FIG. 8 are ~~four~~ three types of content scanners: a scanner for HTML content,

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

a scanner for JavaScript content, and a scanner for URI content. An advantage of the present invention is the ability to generate such a multitude of content scanners within a unified framework.

Please amend page 35, 2nd full paragraph of the original specification as follows:

[00120] When the client downloads content from the Internet it preferably creates a pool of thread objects. Each thread object stores its ARB scanner factory instance 750 as member data. Whenever a thread object has content to parse, it requests an appropriate ARB scanner 760 from its ARB scanner factory object 750. Then, using the ARB scanner interface, the thread passes content and calls the requisite API functions to scan and process the content. Preferably, when the thread finishes scanning the content, it returns the ARB scanner instance 760 to its ARB scanner factory 750, to enable pooling ~~[[to]]~~ the ARB scanner for later re-use.

Please amend page 36, 1st full paragraph of the original specification as follows:

[00125] Desktop computer 900 preferably includes a network traffic probe 920, which generally passes incoming network traffic to its destination, be it a browser, e-mail client or other Internet application. However, in accordance with a preferred embodiment of the present invention, network traffic probe 920 selectively diverts incoming network traffic to ARB scanner 930. ARB scanner 930 scans and analyzes content to detect the presence of potential exploits. To this end, desktop computer 900 preferably maintains a database 940 of coded exploit rules in the form of

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

deterministic or non-deterministic finite automata, which perform pattern matches appropriate to exploits under consideration. If ARB scanner 930 does not detect a match with a potential exploit, then the content is routed to its destination. Otherwise, if ARB scanner 930 detects the presence of potential exploits, then the suspicious content is passed to content ~~blocked~~ blocker 950, which removes or inoculates such content.

Please amend page 36, 2nd full paragraph of the original specification as follows:

[00126] In order to keep exploit rule database 940 current, desktop computer ~~[[800]]~~ 900 preferably includes a rules update manager 960, which periodically receives modified rules and new rules over the Internet, and updates database 940 accordingly.

Please amend page 36, 5th full paragraph of the original specification as follows:

[00129] The ability to distribute ARB scanners among desktop computers residing at the periphery of a network is of advantage to the entire network. Scanning results for mobile code, i.e., security profiles, are centrally cached at a network server or gateway, such as rules update server 1010, indexed according to IDs, such as ~~[[a]]~~ hash values, for the mobile code; and made available to other desktop computers within the network. Use of IDs for caching security profiles is described in applicant's US Patent No. ~~6,804,780~~ 6,804,780, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables."

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

Please amend page 37, 2nd full paragraph of the original specification as follows:

[00131] When ARB scanner 930 receives content to scan, it first checks if a security profile for the content is already available in cache. If so, then ARB scanner 930 does not need to scan the content, and can use the security profile previously derived by itself or by an ARB scanner from another desktop computer. Thus it may be appreciated that desktop computers mutually benefit one another from the security profiles that they generate and share among themselves.

Please amend page 39, 3rd full paragraph of the original specification as follows:

[00140] Reference is now made to FIG. 12, which is a simplified block diagram of an integrated content scanner including a general behavioral scanner and a sandbox scanner, in accordance with a preferred embodiment of the present invention. As shown in FIG. 12, incoming content is received by ARB scanner 1210. ARB scanner 1210 derives an ID for the content and checks a local security profile cache 1220 to determine whether or not a security profile for the content already resides in local cache. If so, then ARB scanner 1210 does not need to derive the security profile, saving significant processing time. If not, then ARB scanner 1210 performs a general behavioral scan of the content, using an adaptive rule-based analysis. ARB analysis is generally carried out without executing the content being analyzed. Such analysis often identifies conditionally malicious code; i.e., code that is or is not malicious depending upon values of operational data that are determined at run-time. Without

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

further information, such content is generally blocked unconditionally in order not to compromise system security. However, such blocking of content with conditionally malicious code is a source of unwanted over-blocking.

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

1. (currently amended) A security system for scanning content within a computer, comprising:

a network interface, housed within a computer, for receiving content from the Internet on its destination to an Internet application running on the computer;

a database of behavioral rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are potentially malicious, wherein the behavioral rules describe computer exploits as logical combinations of patterns of program code constructs;

a rule-based content scanner that communicates with said database of behavioral rules, operatively coupled with said network interface, for scanning content received by said network interface to recognize the presence of ~~potential~~ computer exploits therewithin;

a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting content from its intended destination to said rule-based content scanner; and

a rule update manager that communicates with said database of behavioral rules, for updating said database of behavioral rules periodically to incorporate new behavioral rules that are made available.

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

2. (currently amended) The security system of claim **1** wherein said database of behavioral rules stores behavioral rules in the form of pattern-matching engines.

3. (original) The security system of claim **2** wherein the pattern-matching engines are deterministic finite automata.

4. (original) The security system of claim **2** wherein the pattern-matching engines are non-deterministic finite automata.

5. (currently amended) The security system of claim **1** further comprising a content blocker, operatively coupled to said rule-based content scanner, for preventing content having a ~~potential~~ computer exploit that was recognized by said rule-based content scanner from reaching its intended destination.

6. (original) The system of claim **1** wherein the content received from the Internet by said network interface is HTTP content.

7. (original) The system of claim **1** wherein the content received from the Internet by said network interface is HTTPS content.

8. (original) The system of claim **1** wherein the content received from the Internet by said network interface is FTP content

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

9. (original) The system of claim **1** wherein the content received from the Internet by said network interface is SMTP content

10. (original) The system of claim **1** wherein the content received from the Internet by said network interface is POP3 content

11. (original) The system of claim **1** wherein the destination Internet application is a web browser.

12. (original) The system of claim **1** wherein the destination Internet application is an e-mail client.

13. (currently amended) A method for scanning content within a computer, comprising:

receiving content from the Internet on its destination to an Internet application;

selectively diverting the received content from its intended destination;

scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of behavioral rules corresponding to computer exploits, computer exploits being portions of program code that are potentially malicious, wherein the behavioral rules describe computer exploits as logical combinations of patterns of program code constructs; and

updating the database of behavioral rules periodically to incorporate new behavioral rules that are made available.

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

14. (currently amended) The method of claim **13** wherein said database of behavioral rules stores behavioral rules in the form of pattern-matching engines.

15. (original) The method of claim **14** wherein the pattern-matching engines are deterministic finite automata.

16. (original) The method of claim **14** wherein the pattern-matching engines are non-deterministic finite automata.

17. (currently amended) The method of claim **13** further comprising preventing content having a potential computer exploit that was recognized by said scanning from reaching its intended destination.

18. (original) The method of claim **13** wherein the content received from the Internet by said network interface is HTTP content.

19. (original) The method of claim **13** wherein the content received from the Internet by said network interface is HTTPS content.

20. (original) The method of claim **13** wherein the content received from the Internet by said network interface is FTP content

21. (original) The method of claim **13** wherein the content received from the Internet by said network interface is SMTP content

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

22. (original) The method of claim **13** wherein the content received from the Internet by said network interface is POP3 content

23. (original) The method of claim **13** wherein the destination Internet application is a web browser.

24. (original) The method of claim **13** wherein the destination Internet application is an e-mail client.

25. (currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving content from the Internet on its destination to an Internet application;

selectively diverting the received content from its intended destination;

scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of behavioral rules corresponding to computer exploits, computer exploits being portions of program code that are potentially malicious, wherein the behavioral rules describe exploits as logical combinations of patterns of program code constructs; and

updating the database of behavioral rules periodically to incorporate new behavioral rules that are made available.

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

REMARKS

Applicants have carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicants have amended claims **1, 2, 5, 13, 14, 17** and **25** to properly claim the present invention. No new matter has been added. Claims **1 - 25** are presented for examination.

On pages 2 – 4 of the Office Action, the Examiner has rejected claims **1, 2, 5, 6, 8 – 13, 17, 18** and **20 – 25** under 35 U.S.C. §102(e) as being anticipated by Freund, U.S. Patent No. 5,987,611 (“Freund”).

On pages 4 and 5 of the Office Action, the Examiner has rejected claims **3, 4, 7, 14 – 16** and **19** under 35 U.S.C. §103(a) as being unpatentable over Freund.

Distinctions between Claimed Invention and U.S. Patent No. 5,987,611 to Freund

Aspects of the subject invention concern diagnosing mobile program code such as JavaScript, VBScript, URI, URL and HTML, to identify potential exploits within the code. The content scanner that performs the diagnostics receives incoming content in the form of byte source code, such as JavaScript and VBScript, and generates as output a profile, which is a list of potential exploits and their respective locations within the code. The

Attorney's Docket No.: FIN0001C1CIP3CIP1*PATENT*

content scanner is provided with parsing rules that characterize syntactical constructs of the source code in terms of patterns of tokens, and analyzer rules that characterize potential exploits. The profile is checked against a security policy to decide whether or not to block the incoming content.

Freund describes client-based monitoring and filtering of Internet access, based on access rules (element **570** of **FIG. 5**). Access rules include criteria such as total time a user can be connected to the Internet, time a user can interactively use the Internet, a list of applications that a user can or cannot use in order to access the Internet, a list of URLs that a user application can or cannot access, and a list of protocols that a user application can or cannot use (Freund/ col. 3, line 51 – col. 4, line 28; col. 12, line 45 – col. 13, line 22; col. 23, line 66 – col. 24, line 15; **FIGS. 7A** and **7B**).

In distinction to Freund, the rules used in the subject claimed invention are parser rules and analyzer rules, which describe program source code exploits in terms of logical combinations of constructs of a specific programming language (original specification/ pars. 11, 55, 56, 66, 67, 81, 82 and 103). The rules used in Freund are Internet access rules, which limit a user's use of the Internet.

In order to further clarify this distinction, applicants have amended the term "rules" to behavioral rules, to distinguish them from the access rules of Freund. Applicants have further added the limitations that exploits are portions of program code that are potentially malicious, and that the behavioral rules describe exploits as logical combinations of patterns of program code constructs.

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

Response to Examiner's Arguments

The rejections of the claims **1** – **25** on pages 2 - 5 of the Office Action will now be dealt with specifically.

As to amended independent claim **1** for a security system, applicant respectfully submits that the limitations in claim **1** of

"a database of behavioral rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are potentially malicious, wherein the behavioral rules describe computer exploits as logical combinations of patterns of program code constructs", and

"a rule-based content scanner that communicates with said database of behavioral rules, operatively coupled with said network interface, for scanning content received by said network interface to recognize the presence of computer exploits therewithin" are neither shown nor suggested in Freund.

In rejecting claim **1**, the Examiner has cited Freund, element **570** of **FIG. 5** as teaching a database of rules corresponding to computer exploits, and Freund, col. 29, line 54 – col. 30, line 10 as teaching scanning of content to recognize exploits. Applicants respectfully submit that the rules described in Freund are access rules that govern Internet access (Freund/ col. 3, line 62; col. 4, line 7; col. 12, line 56; col. 13, line 1; col. 23, line 65 – col. 24, line 20; col. 32, lines 48 and 49), such as total time a user can be connected to the Internet, time a user can interactively use the Internet, applications a user can or cannot use in order to access the Internet, URLs that a user application can or cannot access, and protocols and protocol components that a user application can or cannot

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

use (Freund/ col. 4, lines 8 – 17; **FIGS. 7A – 7K**). With regard to protocol components specifically, Freund at col. 29, line 54 – col. 30, line 10 describes parsing contents of an HTML page for components including (a) Java and ActiveX (<APPLET> and <OBJECT> tags), (b) Netscape plug-ins (<EMBED> tag), and (c) JavaScript and VBScript (<SCRIPT> tag). Freund's access rules determine whether or not the user/workstation has permission to use such components (Freund/ steps **1220**, **1221** and **1222** of **FIG. 12C**). However, Freund's access rules do not describe how to recognize exploits within such components; i.e., within the Java program code, the ActiveX program code, the plug-in program code, the JavaScript program code and the VBScript program code that the user/workstation is trying to access. Instead, Freund simply denies access altogether.

Thus using Freund, for example, a user may either be allowed unconditional access to all JavaScript, or denied access to all JavaScript; whereas using the claimed invention, each JavaScript is scanned for the presence of potentially malicious behavior and then conditionally allowed or denied.

Because claims **2 – 12** depend from claim **1** and include additional features, applicants respectfully submit that claims **2 - 12** are not anticipated or rendered obvious by Freund.

Accordingly claims **1 – 12** are deemed to be allowable.

As to amended independent method claim **13** and amended independent claim **25** for a computer-readable storage medium, applicants respectfully submit that the limitation in claims **13** and **25** of

"scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of behavioral rules

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

corresponding to computer exploits, computer exploits being portions of program code that are potentially malicious, wherein the behavioral rules describe computer exploits as logical combinations of patterns of program code constructs"

is neither shown nor suggested in Freund.

The Examiner has rejected claims **13** and **25** on the same grounds as the claim **1** rejection, and applicants arguments above apply to the rejection of these claims as well.

Because claims **14** – **24** depend from claim **13** and include additional features, applicants respectfully submit that claims **14** - **24** are not anticipated or rendered obvious by Freund.

Accordingly claims **13** – **25** are deemed to be allowable.

Support for New and Amended Claims in Original Specification

Amended independent claims **1**, **12** and **25** include the limitation of behavioral rules that describe computer exploits as logical combinations of patterns of program code constructs. This limitation is supported in the original specification at least at pars. 11, 55, 56, 66, 67, 81, 82 and 103.

Attorney's Docket No.: FIN0001C1CIP3CIP1

PATENT

CONCLUSION

The undersigned representative respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that the prosecution might be advanced by discussing the application with the undersigned representative, in person or over the telephone, we welcome the opportunity to do so. In addition, if any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account 50-4402.

Respectfully submitted,

Date: November 4, 2008
KING & SPALDING LLP
1700 Pennsylvania Ave., NW
Suite 200
Washington, DC 20006
(202) 737-0500

By: /Dawn-Marie Bey - 44, 442/
Dawn-Marie Bey
Registration No. 44,442



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. |
|---|-------------|----------------------|---------------------|------------------|
| 11/009,437 | 12/09/2004 | Moshe Rubin | 60644-8005.US02 | 5071 |
| 22918 | 7590 | 09/05/2008 | EXAMINER | |
| PERKINS COIE LLP P.O. BOX 1208 SEATTLE, WA 98111-1208 | | | WILLIAMS, JEFFERY L | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2137 | |
| | | | MAIL DATE | DELIVERY MODE |
| | | | 09/05/2008 | 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.

Application/Control Number: 11/009,437
Art Unit: 2137

Page 2

1 **DETAILED ACTION**

2

3 Claims 1 – 25 are rejected.

4

5 ***Claim Rejections - 35 USC § 102***

6 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that
7 form the basis for the rejections under this section made in this Office action:

8 A person shall be entitled to a patent unless –

9 (e) the invention was described in (1) an application for patent, published under section 122(b), by
10 another filed in the United States before the invention by the applicant for patent or (2) a patent
11 granted on an application for patent by another filed in the United States before the invention by the
12 applicant for patent, except that an international application filed under the treaty defined in section
13 351(a) shall have the effects for purposes of this subsection of an application filed in the United States
14 only if the international application designated the United States and was published under Article 21(2)
15 of such treaty in the English language.

16
17 **Claims 5, 6, 8 –12, 13, 17, 18, and 20 – 25 are rejected under 35 U.S.C. 102(e)**
18 **as being anticipated by Freund, U.S. Patent, 5,987,611.**

19

20 Regarding claim 1, Freund discloses:

21 *a network interface, housed within a computer, for receiving content from the*
22 *Internet on its destination to an Internet application running on the computer (Freund,*
23 *fig. 2:220);*

24 *a database of rules corresponding to computer exploits, stored within the*
25 *computer (Fruend, fig. 5:570); a rule-based content scanner that communicates with*
26 *said database of rules, for scanning content to recognize the presence of potential*
27 *exploits therewithin (Fruend, 29:54-30:10); a network traffic probe, operatively coupled*

Application/Control Number: 11/009,437
Art Unit: 2137

Page 3

1 *to said network interface and to said rule-based content scanner, for selectively*
2 *diverting content from its intended destination to said rule-based content scanner*
3 *(Freund, fig. 3a:311);*
4 *and a rule update manager that communicates with said database of rules, for*
5 *updating said database of rules periodically to incorporate new rules that are made*
6 *available (Freund, 21:33-40).*

7

8 Regarding claim 2, Freund discloses:

9 wherein said database of rules stores rules in the form of pattern-matching
10 engines (Freund, 29:54-30:10). Herein, Freund discloses that the rules enable the
11 driver or parser to operate according to a particular manner.

12

13 Regarding claim 5, Freund discloses:

14 *a content blocker, operatively coupled to said rule-based content scanner, for*
15 *preventing a potential exploit that was recognized by said rule-based content scanner*
16 *from reaching its intended destination (Freund, 15:22-16:7).*

17

18 Regarding claims 6, 8 – 10, Freund discloses:

19 *wherein the content received from the Internet by said network interface is HTTP,*
20 *FTP, SMTP, POP3 content (Freund, 23:44-55).*

21

22 Regarding claims 11 and 12, Freund discloses:

Application/Control Number: 11/009,437
Art Unit: 2137

Page 4

1 *wherein the destination Internet application is a web browser; wherein the*
2 *destination Internet application is an e-mail client (12:18-42).*

3

4 Regarding claims 13, 17, 18, 20 – 25, they are rejected, at least, for the same
5 reasons as claims 1, 5, 6, 8 – 12.

6

7

Claim Rejections - 35 USC § 103

8

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

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

16

17 **Claims 7 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable**
18 **over Freund, U.S. Patent, 5,987,611.**

19

20 Regarding claims 7 and 19, Freund discloses that the system is flexible so as to
21 support a plurality of protocols (Freund, 12:18-42). While Freund discloses supporting
22 existing protocols such as HTTP, Freund does not appear to explicitly state that the
23 system may support secure HTTP. However, it would have been obvious to one of
24 ordinary skill in the art to employ support for the secure HTTP because one of ordinary
25 skill in the art would have been motivated by increased flexibility of the system.

26

Application/Control Number: 11/009,437
Art Unit: 2137

Page 5

1 Regarding claims 3, 4, and 14 – 16, Freund discloses parsing means for pattern
2 matching, but does not appear to disclose DFA or NDFA. However, the examiner notes
3 that it was well known in the art for DFA and NDFA to be used as engines for pattern
4 matching (e.g. see admission by the applicant, Applicant's specification, par. 73).

5

6

7

Conclusion

8

9 The prior art made of record and not relied upon is considered pertinent to
10 applicant's disclosure:

11 **See Notice of References Cited.**

12

13 A shortened statutory period for reply is set to expire **3** months (not less than 90
14 days) from the mailing date of this communication.

15 Any inquiry concerning this communication or earlier communications from the
16 examiner should be directed to Jeffery Williams whose telephone number is (571) 272-
17 7965. The examiner can normally be reached on 8:30-5:00.

18 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
19 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone
20 number for the organization where this application or proceeding is assigned is (703)
21 872-9306.

Application/Control Number: 11/009,437
Art Unit: 2137

Page 6

1 Information regarding the status of an application may be obtained from the
2 Patent Application Information Retrieval (PAIR) system. Status information for
3 published applications may be obtained from either Private PAIR or Public PAIR.
4 Status information for unpublished applications is available through Private PAIR only.
5 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
6 you have questions on access to the Private PAIR system, contact the Electronic
7 Business Center (EBC) at 866-217-9197 (toll-free).

8

9

10 J. Williams
11 AU 2137

12

13 /Emmanuel L. Moise/

14 Supervisory Patent Examiner, Art Unit 2137

15

UNITED STATES PATENT APPLICATION

FOR

**Method and System for Adaptive Rule-Based Content Scanners for
Desktop Computers**

Inventors:

Moshe Rubin
Moshe Matitya
Artem Melnick
Shlomo Touboul
Alexander Yermakov
Amit Shaked

Please direct communications to:

Marc A. Sockol, Esq.
SQUIRE, SANDERS & DEMPSEY, L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043

EXPRESS MAIL CERTIFICATE OF MAILING

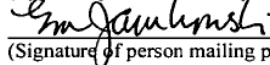
"Express Mail" mailing label number: EV 609 138 904 US

Date of Deposit: December 9, 2004

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Eileen M. Janikowski

(Typed or printed name of person mailing paper or fee)



(Signature of person mailing paper or fee)

December 9, 2004

(Date signed)

**Method and System for Adaptive Rule-Based
Content Scanners for Desktop Computers**

CROSS REFERENCES TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of assignee's pending application U.S. Serial No. 10/930,884, filed on August 30, 2004, entitled "Method and System for Adaptive Rule-Based Content Scanners," which is a continuation-in-part of assignee's pending application U.S. Serial No. 09/539,667, filed on March 30, 2000, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables," which is a continuation of assignee's patent application U.S. Serial No. U.S. Ser. No. 08/964,388, filed on 6 November 1997, now U.S. Patent No. 6,092,194, also entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables."

FIELD OF THE INVENTION

[0002] The present invention relates to network security, and in particular to scanning of mobile content for exploits.

BACKGROUND OF THE INVENTION

[0003] Conventional anti-virus software scans a computer file system by searching for byte patterns, referred to as signatures that are present within known viruses. If a virus signature is discovered within a file, the file is designated as infected.

[0004] Content that enters a computer from the Internet poses additional security threats, as such content executes upon entry into a client computer, without being saved into the computer's file system. Content such as JavaScript and VBScript is executed by an Internet browser, as soon as the content is received within a web page.

[0005] Conventional network security software also scans such mobile content by searching for heuristic virus signatures. However, in order to be as protective as possible, virus signatures for mobile content tend to be over-conservative, which results in significant over-blocking of content. Over-blocking refers to false positives; i.e., in addition to blocking

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

of malicious content, prior art technologies also block a significant amount of content that is not malicious.

[0006] Another drawback with prior art network security software is that it is unable to recognize combined attacks, in which an exploit is split among different content streams. Yet another drawback is that prior art network security software is unable to scan content containers, such as URI within JavaScript.

[0007] All of the above drawbacks with conventional network security software are due to an inability to diagnose mobile code. Diagnosis is a daunting task, since it entails understanding incoming byte source code. The same malicious exploit can be encoded in an endless variety of ways, so it is not sufficient to look for specific signatures.

[0008] Nevertheless, in order to accurately block malicious code with minimal over-blocking, a thorough diagnosis is required.

SUMMARY OF THE DESCRIPTION

[0009] The present invention enables behavioral analysis of content. As distinct from prior art approaches that search for byte patterns, the approach of the present invention is to analyze incoming content in terms of its programmatic behavior. Behavioral analysis is an automated process that parses and diagnoses a software program, to determine if such program can carry out an exploit.

[0010] The present invention provides a method and system for scanning content that includes mobile code, to produce a diagnostic analysis of potential exploits within the content. The present invention is preferably used within a network gateway or proxy, to protect an intranet against viruses and other malicious mobile code.

[0011] The content scanners of the present invention are referred to as adaptive rule-based (ARB) scanners. An ARB scanner is able to adapt itself dynamically to scan a specific type of content, such as inter alia JavaScript, VBScript, URI, URL and HTTP. ARB scanners differ from prior art scanners that are hard-coded for one particular type of content. In distinction, ARB scanners are data-driven, and can be enabled to scan any specific type of content by providing appropriate rule files, without the need to modify source code. Rule files are text files that describe lexical characteristics of a particular language. Rule files for a language describe character encodings, sequences of characters that form lexical constructs of the language, referred to as tokens, patterns of tokens that form syntactical constructs of program code, referred to as parsing rules, and patterns of tokens that correspond to potential exploits, referred to as analyzer rules. Rules files thus serve as adaptors, to adapt an ARB content scanner to a specific type of content.

[0012] The present invention also utilizes a novel description language for efficiently describing exploits. This description language enables an engineer to describe exploits as logical combinations of patterns of tokens.

[0013] Thus it may be appreciated that the present invention is able to diagnose incoming content for malicious behavior. As such, the present invention achieves very accurate blocking of content, with minimal over-blocking as compared with prior art scanning technologies.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

[0014] There is thus provided in accordance with a preferred embodiment of the present invention a security system for scanning content within a computer, including a network interface, housed within a computer, for receiving content from the Internet on its destination to an Internet application running on the computer, a database of rules corresponding to computer exploits, stored within the computer, a rule-based content scanner that communicates with said database of rules, for scanning content to recognize the presence of potential exploits therewithin, a network traffic probe, operatively coupled to the network interface and to the rule-based content scanner, for selectively diverting content from its intended destination to the rule-based content scanner, and a rule update manager that communicates with said database of rules, for updating said database of rules periodically to incorporate new rules that are made available.

[0015] There is moreover provided in accordance with a preferred embodiment of the present invention a method for scanning content within a computer, including receiving content from the Internet on its destination to an Internet application, selectively diverting the received content from its intended destination, scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of rules corresponding to computer exploits, and updating the database of rules periodically to incorporate new rules that are made available.

[0016] There is further provided in accordance with a preferred embodiment of the present invention a computer-readable storage medium storing program code for causing a computer to perform the steps of receiving content from the Internet on its destination to an Internet application, selectively diverting the received content from its intended destination, scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of rules corresponding to computer exploits, and updating the database of rules periodically to incorporate new rules that are made available.

[0017] There is yet further provided in accordance with a preferred embodiment of the present invention, a method for network security, including scanning content received over a computer network for potential malicious code, the intended destination of the content being a software application, including deriving a hash value for the received content, querying a

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

local security cache for the presence of the hash value, the local security cache storing hash values for content and corresponding security profiles, whereby security profiles identify potentially malicious code within content, and if the querying is affirmative, then retrieving a security policy for the content from the local security cache, else if the querying is not affirmative, then deriving a security profile for the received content, storing the hash value and the derived security policy in the local security cache, and transmitting the hash value and the security policy to a central security cache, and periodically updating the local security cache with hash values and corresponding security profiles from the central security cache.

[0018] There is additionally provided in accordance with a preferred embodiment of the present invention a network security system including a plurality of inter-connected computers within a network, each of the plurality of computers including a local security cache that stores hash values for content and corresponding content security profiles, whereby security profiles identify potentially malicious code within content, a scanner that communicates bi-directionally with the local security cache, for (i) examining incoming content and deriving a hash value therefor, the intended destination of the content being a software application; (ii) querying the local security cache for the presence of the derived hash value; and (iii) examining incoming content and deriving a security profile therefor, and a central security cache storing hash values for content and corresponding content security profiles, to which hash values and corresponding security profiles are received from the plurality of inter-connected computers, and from which updated hash values and corresponding security profiles are transmitted to the plurality of local security caches.

[0019] There is moreover provided in accordance with a preferred embodiment of the present invention a computer-readable storage medium storing program code for causing a computer to perform the steps of scanning content received over a computer network for potential malicious code, the intended destination of the content being a software application, including deriving a hash value for the received content, querying a local security cache for the presence of the hash value, the local security cache storing hash values for content and corresponding security profiles, whereby security profiles identify potentially malicious code within content, and if the querying is affirmative, then retrieving a security policy for the

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

content from the local security cache, else if the querying is not affirmative, then deriving a security profile for the received content, storing the hash value and the derived security policy in the local security cache, and transmitting the hash value and the security policy to a central security cache, and periodically updating the local security cache with hash values and corresponding security profiles from the central security cache.

[0020] There is further provided in accordance with a preferred embodiment of the present invention a network security system including a first scanner that analyzes incoming content under general operational conditions, without executing the content, and derives a security profile for the content that identifies conditionally malicious code therein, which is malicious or non-malicious depending upon values of operational data, and a second scanner, connected in series with the first scanner, that analyzes the content under specific operational conditions corresponding to specific values of the operational data, by executing the content, and modifies the security profile for the content if the conditionally malicious code identified in the security profile is found to be malicious for the specific values of the operational data.

[0021] There is yet further provided in accordance with a preferred embodiment of the present invention a method for network security, including analyzing incoming content under general operational conditions, without executing the content, deriving a security profile for the content that identifies conditionally malicious code therein, which is malicious or non-malicious depending upon values of operational data, if the security profile identifies conditionally malicious code within the content, then further analyzing the content under specific operational conditions corresponding to specific values of the operational data, by executing the content, and modifying the security profile for the content if the conditionally malicious code identified in the security profile is found to be malicious for the specific values of the operational data, so as to identify the conditionally malicious code as being malicious.

[0022] There is yet further provided in accordance with a preferred embodiment of the present invention a computer-readable storage medium storing program code for causing a computer to perform the steps of analyzing incoming content under general operational conditions, without executing the content, deriving a security profile for the content that

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

identifies conditionally malicious code therein, which is malicious or non-malicious depending upon values of operational data, if the security profile identifies conditionally malicious code within the content, then further analyzing the content under specific operational conditions corresponding to specific values of the operational data, by executing the content, and modifying the security profile for the content if the conditionally malicious code identified in the security profile is found to be malicious for the specific values of the operational data, so as to identify the conditionally malicious code as being malicious.

[0023] Additional claims for future consideration are listed below.

26. A method for network security, comprising:
scanning content received over a computer network for potential malicious code, the intended destination of the content being a software application, comprising:
deriving a hash value for the received content;
querying a local security cache for the presence of the hash value, the local security cache storing hash values for content and corresponding security profiles, whereby security profiles identify potentially malicious code within content; and
if said querying is affirmative, then:
retrieving a security policy for the content from the local security cache;
else if said querying is not affirmative, then:
deriving a security profile for the received content;
storing the hash value and the derived security policy in the local security cache; and
transmitting the hash value and the security policy to a central security cache; and
periodically updating the local security cache with hash values and corresponding security profiles from the central security cache.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

27. The method of claim 26 wherein the intended destination of the content is an Internet web browser.

28. The method of claim 26 wherein the intended destination of the content is an e-mail client.

29. The method of claim 26 further comprising modifying the received content so as to remove potentially malicious code identified in the content security profile, if the security profile identifies such potentially malicious code.

30. The method of claim 26 further comprising blocking the received content from reaching its intended destination, if the security profile of the content identifies potentially malicious code.

31. A network security system comprising:
a plurality of inter-connected computers within a network, each of said plurality of computers comprising:

a local security cache that stores hash values for content and corresponding content security profiles, whereby security profiles identify potentially malicious code within content;

a scanner that communicates bi-directionally with said local security cache, for (i) examining incoming content and deriving a hash value therefor, the intended destination of the content being a software application; (ii) querying the local security cache for the presence of the derived hash value; and (iii) examining incoming content and deriving a security profile therefor; and

a central security cache storing hash values for content and corresponding content security profiles, to which hash values and corresponding security profiles are received from said plurality of inter-connected computers, and from which updated hash values and corresponding security profiles are transmitted to said plurality of local security caches.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

32. The network security system of claim 31 wherein the intended destination of the content is an Internet web browser.

33. The network security system of claim 31 wherein the intended destination of the content is an e-mail client.

34. The network security system of claim 31 further comprising a content blocker, for modifying the received content so as to remove potentially malicious code identified in the content security profile, if the security profile identifies such potentially malicious code.

35. The network security system of claim 31 further comprising a content blocker, for blocking the received content from reaching its intended destination, if the security profile of the content identifies potentially malicious code.

36. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

scanning content received over a computer network for potential malicious code, the intended destination of the content being a software application, comprising:

deriving a hash value for the received content;

querying a local security cache for the presence of the hash value, the local security cache storing hash values for content and corresponding security profiles, whereby security profiles identify potentially malicious code within content; and

if said querying is affirmative, then:

retrieving a security policy for the content from the local security cache;

else if said querying is not affirmative, then:

deriving a security profile for the received content;

storing the hash value and the derived security policy in the local security cache; and

transmitting the hash value and the security policy to a central security cache; and

periodically updating the local security cache with hash values and corresponding security profiles from the central security cache.

37. A network security system comprising:

a first scanner that analyzes incoming content under general operational conditions, without executing the content, and derives a security profile for the content that identifies conditionally malicious code therein, which is malicious or non-malicious depending upon values of operational data;

a second scanner, connected in series with said first scanner, that analyzes the content under specific operational conditions corresponding to specific values of the operational data, by executing the content, and modifies the security profile for the content if the conditionally malicious code identified in the security profile is found to be malicious for the specific values of the operational data.

38. The network security system of claim 37 wherein said first scanner is an adaptive rule-based (ARB) scanner.

39. The network security system of claim 38 wherein said second scanner is a sandbox scanner that executes the incoming content in a protected environment, so that the content cannot access critical system data.

40. A method for network security system, comprising:

analyzing incoming content under general operational conditions, without executing the content;

deriving a security profile for the content that identifies conditionally malicious code therein, which is malicious or non-malicious depending upon values of operational data;

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

if the security profile identifies conditionally malicious code within the content, then further analyzing the content under specific operational conditions corresponding to specific values of the operational data, by executing the content; and

modifying the security profile for the content if the conditionally malicious code identified in the security profile is found to be malicious for the specific values of the operational data, so as to identify the conditionally malicious code as being malicious.

41. The method of claim 41 wherein said further analyzing executes the incoming content in a protected environment, so that the content cannot access critical system data.

42. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

analyzing incoming content under general operational conditions, without executing the content;

deriving a security profile for the content that identifies conditionally malicious code therein, which is malicious or non-malicious depending upon values of operational data;

if the security profile identifies conditionally malicious code within the content, then further analyzing the content under specific operational conditions corresponding to specific values of the operational data, by executing the content; and

modifying the security profile for the content if the conditionally malicious code identified in the security profile is found to be malicious for the specific values of the operational data, so as to identify the conditionally malicious code as being malicious.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0024] The present invention will be more fully understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:
- [0025] FIG. 1 is a simplified block diagram of an overall gateway security system that uses an adaptive rule-based (ARB) content scanner, in accordance with a preferred embodiment of the present invention;
- [0026] FIG. 2 is a simplified block diagram of an adaptive rule-based content scanner system, in accordance with a preferred embodiment of the present invention;
- [0027] FIG. 3 is an illustration of a simple finite state machine for detecting tokens “a” and “ab”, used in accordance with a preferred embodiment of the present invention;
- [0028] FIG. 4A is an example of a non-deterministic finite automaton (NFA) for matching a pattern of tokens;
- [0029] FIG. 4B is an example of a deterministic finite automaton (DFA) which is equivalent to the NFA of FIG. 4A;
- [0030] FIG. 5 is an illustration of a simple finite state machine for a pattern, used in accordance with a preferred embodiment of the present invention;
- [0031] FIG. 6 is a simplified flowchart of operation of a parser for a specific content language within an ARB content scanner, in accordance with a preferred embodiment of the present invention;
- [0032] FIG. 7 is a simplified block diagram of a system for serializing binary instances of ARB content scanners, transmitting them to a client site, and regenerating them back into binary instances at the client site, in accordance with a preferred embodiment of the present invention;
- [0033] FIG. 8 illustrates a representative hierarchy of objects created by a builder module, in accordance with a preferred embodiment of the present invention;
- [0034] FIG. 9 is a simplified block diagram of a desktop computer implementation of an ARB content scanner, in accordance with a preferred embodiment of the present invention;
- and

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

[0035] FIG. 10 is a simplified block diagram of a rule server that updates rule databases for the desktop computer of FIG. 9, in accordance with a preferred embodiment of the present invention;

[0036] FIG. 11 is a simplified block diagram of a network security system that takes advantage of distributed ARB scanners to populate a central security profile cache, in accordance with a preferred embodiment of the present invention; and

[0037] FIG. 12 is a simplified block diagram of an integrated content scanner including a general behavioral scanner and a sandbox scanner, in accordance with a preferred embodiment of the present invention.

LIST OF APPENDICES

[0038] Appendix A is a source listing of an ARB rule file for the JavaScript language, in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION

[0039] The present invention concerns scanning of content that contains mobile code, to protect an enterprise against viruses and other malicious code.

[0040] Reference is now made to FIG. 1, which is a simplified block diagram of an overall gateway security system that uses an adaptive rule-based (ARB) content scanner, in accordance with a preferred embodiment of the present invention. Shown in FIG. 1 is a network gateway 110 that acts as a conduit for content from the Internet entering into a corporate intranet, and for content from the corporate intranet exiting to the Internet. One of the functions of network gateway 110 is to protect client computers 120 within the corporate intranet from malicious mobile code originating from the Internet. Mobile code is program code that executes on a client computer. Mobile code can take many diverse forms, including inter alia JavaScript, Visual Basic script, HTML pages, as well as a Uniform Resource Identifier (URI).

[0041] Mobile code can be detrimental to a client computer. Mobile code can access a client computer's operating system and file system, can open sockets for transmitting data to and from a client computer, and can tie up a client computer's processing and memory resources. Such malicious mobile code cannot be detected using conventional anti-virus scanners, which scan a computer's file system, since mobile code is able to execute as soon as it enters a client computer from the Internet, before being saved to a file. Thus it may be appreciated that the security function of network gateway 110 is critical to a corporate intranet.

[0042] Many examples of malicious mobile code are known today. Portions of code that are malicious are referred to as exploits. For example, one such exploit uses JavaScript to create a window that fills an entire screen. The user is then unable to access any windows lying underneath the filler window. The following sample code shows such an exploit.

EXAMPLE EXPLOIT

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
<TITLE>BID-3469</TITLE>
<SCRIPT>
```

```

op=window.createPopup();
s='<body>foobar</body>';
op.document.body.innerHTML=s;

function oppop()
{
  if (!op.isOpen)
    op.show(0,0, screen.width, screen.height, document.body);
}

function doit ()
{
  oppop();
  setInterval("window.focus(); {opop();}",10);
}
</SCRIPT>
</HEAD>
<BODY>
<H1>BID-3469</H1>
<FORM method=POST action="">
<INPUT type="button" name="btnDoIt" value="Do It" onclick="doit()">
</FORM>
</BODY>
</HTML>

```

[0043] The command

```
op.show(0,0, screen.width, screen.height, document.body)
```

is responsible for opening a window that fills the entire screen. It may be appreciated that there are many equivalents to such command. For example, the section of code

```

{
  w = screen.width;
  h = screen.height;
  op.show(0,0, w, h, document.body);
}

```

performs the same action of opening a window that fills the entire screen; as also does the section of code

```

{
  a = screen.width;
  b = screen.height;
  w = a;
  h = b;
  op.show(0,0, w, h, document.body);
}

```

In distinction, although it appears similar, the section of code

```
{
```

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

```
w = screen.width;  
h = screen.height;  
w = 10;  
h = 10;  
op.show(0,0, w, h, document.body);  
}
```

does not fill the screen, and may be part of non-malicious content.

[0044] Furthermore, each variation of code section takes on a different binary form when streamed within JavaScript, and thus requires a different signature for detection. Thus it may be appreciated that conventional signature-based anti-virus detection is incapable of coping with the unlimited number of variants of a virus. Instead, what is required, even for known exploits, is a behavioral approach that analyses content based on its behavior instead of its binary structure.

[0045] In accordance with a preferred embodiment of the present invention, network gateway includes a content scanner 130, whose purpose is to scan mobile code and identify potential exploits. Content scanner 130 receives as input content containing mobile code in the form of byte source, and generates a security profile for the content. The security profile indicates whether or not potential exploits have been discovered within the content, and, if so, provides a diagnostic list of one or more potential exploits and their respective locations within the content.

[0046] Preferably, the corporate intranet uses a security policy to decide whether or not to block incoming content based on the content's security profile. For example, a security policy may block content that may be severely malicious, say, content that accesses an operating system or a file system, and may permit content that is less malicious, such as content that can consume a user's computer screen as in the example above. The diagnostics within a content security profile are compared within the intranet security policy, and a decision is made to allow or block the content. When content is blocked, one or more alternative actions can be taken, such as replacing suspicious portions of the content with innocuous code and allowing the modified content, and sending a notification to an intranet administrator.

[0047] Scanned content and their corresponding security profiles are preferably stored within a content cache 140. Preferably, network gateway checks if incoming content is already resident in cache 140, and, if so, bypasses content scanner 130. Use of cache 140 saves content scanner 130 the task of re-scanning the same content.

[0048] Alternatively, a hash value of scanned content, such as an MD5 hash value, can be cached instead of caching the content itself. When content arrives at scanner 130, preferably its hash value is computed and checked against cached hash values. If a match is found with a cached hash value, then the content does not have to be re-scanned and its security profile can be obtained directly from cache.

[0049] Consider, for example, a complicated JavaScript file that is scanned and determined to contain a known exploit therewithin. An MD5 hash value of the entire JavaScript file can be stored in cache, together within a security profile indicating that the JavaScript file contains the known exploit. If the same JavaScript file arrives again, its hash value is computed and found to already reside in cache. Thus, it can immediately be determined that the JavaScript file contains the known exploit, without re-scanning the file.

[0050] It may be appreciated by those skilled in the art that cache 140 may reside at network gateway 110. However, it is often advantageous to place cache 140 as close as possible to the corporate intranet, in order to transmit content to the intranet as quickly as possible. However, in order for the security profiles within cache 140 to be up to date, it is important that network gateway 110 notify cache 140 whenever content scanner 130 is updated. Updates to content scanner 130 can occur inter alia when content scanner 130 is expanded (i) to cover additional content languages; (ii) to cover additional exploits; or (iii) to correct for bugs.

[0051] Preferably, when cache 140 is notified that content scanner 130 has been updated, cache 140 clears its cache, so that content that was in cache 140 is re-scanned upon arrival at network gateway 110.

[0052] Also, shown in FIG. 1 is a pre-scanner 150 that uses conventional signature technology to scan content. As mentioned hereinabove, pre-scanner 150 can quickly determine if content is innocuous, but over-blocks on the safe side. Thus pre-scanner 150 is

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

useful for recognizing content that poses no security threat. Preferably, pre-scanner 150 is a simple signature matching scanner, and processes incoming content at a rate of approximately 100 mega-bits per second. ARB scanner 130 performs much more intensive processing than pre-scanner 150, and processes incoming content at a rate of approximately 1 mega-bit per second.

[0053] In order to accelerate the scanning process, pre-scanner 150 acts as a first-pass filter, to filter content that can be quickly recognized as innocuous. Content that is screened by pre-scanner 150 as being potentially malicious is passed along to ARB scanner 130 for further diagnosis. Content that is screened by pre-scanner 150 as being innocuous bypasses ARB scanner 130. It is expected that pre-scanner filters 90% of incoming content, and that only 10% of the content required extensive scanning by ARB scanner 130. As such, the combined effect of ARB scanner 130 and pre-scanner 150 provides an average scanning throughout of approximately 9 mega-bits per second.

[0054] Use of security profiles, security policies and caching is described in applicant's U.S. Patent No. 6,092,194 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, in applicant's U.S. Patent Application Serial No. 09/539,667 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES and filed on 30 March 2000, and in applicant's U.S. Patent Application Serial No. 10/838,889 entitled METHOD AND SYSTEM FOR CACHING AT SECURE GATEWAYS and filed on 3 May 2004

[0055] Reference is now made to FIG. 2, which is a simplified block diagram of an adaptive rule-based content scanner system 200, in accordance with a preferred embodiment of the present invention. An ARB scanner system is preferably designed as a generic architecture that is language-independent, and is customized for a specific language through use of a set of language-specific rules. Thus, a scanner system is customized for JavaScript by means of a set of JavaScript rules, and is customized for HTML by means of a set of HTML rules. In this way, each set of rules acts as an adaptor, to adapt the scanner system to

a specific language. A sample rule file for JavaScript is provided in Appendix A, and is described hereinbelow.

[0056] Moreover, in accordance with a preferred embodiment of the present invention, security violations, referred to as exploits, are described using a generic syntax, which is also language-independent. It is noted that the same generic syntax used to describe exploits is also used to describe languages. Thus, referring to Appendix A, the same syntax is used to describe the JavaScript parser rules and the analyzer exploit rules.

[0057] It may thus be appreciated that the present invention provides a flexible content scanning method and system, which can be adapted to any language syntax by means of a set of rules that serve to train the content scanner how to interpret the language. Such a scanning system is referred to herein as an adaptive rule-based (ARB) scanner. Advantages of an ARB scanner, include inter alia:

- the ability to re-use software code for many different languages;
- the ability to re-use software code for binary content and EXE files;
- the ability to focus optimization efforts in one project, rather than across multiple projects; and
- the ability to describe exploits using a generic syntax, which can be interpreted by any ARB scanner.

[0058] The system of FIG. 2 includes three main components: a tokenizer 210, a parser 220 and an analyzer 230. The function of tokenizer 210 is to recognize and identify constructs, referred to as tokens, within a byte source, such as JavaScript source code. A token is generally a sequence of characters delimited on both sides by a punctuation character, such as a white space. Tokens includes inter alia language keywords, values, names for variables or functions, operators, and punctuation characters, many of which are of interest to parser 220 and analyzer 230.

[0059] Preferably, tokenizer 210 reads bytes sequentially from a content source, and builds up the bytes until it identifies a complete token. For each complete token identified, tokenizer 210 preferably provides both a token ID and the token sequence.

[0060] In a preferred embodiment of the present invention, the tokenizer is implemented as a finite state machine (FSM) that takes input in the form of character codes. Tokens for the language are encoded in the FSM as a sequence of transitions for appropriate character codes, as described hereinbelow with reference to FIG. 3. When a sequence of transitions forms a complete lexical token, a punctuation character, which normally indicates the end of a token, is expected. Upon receiving a punctuation character, the token is complete, and the tokenizer provides an appropriate ID. If a punctuation character is not received, the sequence is considered to be part of a longer sequence, and no ID is provided at this point.

[0061] Reference is now made to FIG. 3, which is an illustration of a simple finite state machine for detecting tokens “a” and “ab”, used in accordance with a preferred embodiment of the present invention. Shown in FIG. 3 are five states, 1 – 5, with labeled and directed transitions therebetween. As tokenizer reads successive characters, a transition is made from a current state to a next state accordingly. State 1 is an entry state, where tokenizer begins. State 4 is a generic state for punctuation. Specifically, whenever a punctuation character is encountered, a transition is made from the current state to state 4. The “a” token is identified whenever a transition is made from state 3 to state 4. Similarly, the “ab” token is identified whenever a transition is made from state 5 to state 4. A generic token, other than “a” and “ab” is identified whenever a transition is made from state 2 to state 4. A punctuation token is identified whenever a transition is made out of state 4.

[0062] Referring back to FIG. 2, tokenizer 210 preferably includes a normalizer 240 and a decoder 250. In accordance with a preferred embodiment of the present invention, normalizer 240 translates a raw input stream into a reduced set of character codes. Normalized output thus becomes the input for tokenizer 210. Examples of normalization rules includes, inter alia

- skipping character ranges that are irrelevant;
- assigning special values to character codes that are irrelevant for the language structure but important for the content scanner;
- translating, such as to lowercase if the language is case-insensitive, in order to reduce input for tokenizer 210;

- merging several character codes, such as white spaces and line ends, into one;
and
- translating sequences of raw bytes, such as trailing spaces, into a single character code.

Preferably, normalizer 240 also handles Unicode encodings, such as UTF-8 and UTF-16.

[0063] In accordance with a preferred embodiment of the present invention, normalizer 240 is also implemented as a finite-state machine. Each successive input is either translated immediately according to normalization rules, or handled as part of a longer sequence. If the sequence ends unexpectedly, the bytes are preferably normalized as individual bytes, and not as part of the sequence.

[0064] Preferably, normalizer 240 operates in conjunction with decoder 250. Preferably, decoder 250 decodes character sequences in accordance with one or more character encoding schemes, including inter alia (i) SGML entity sets, including named sets and numerical sets; (ii) URL escape encoding scheme; (iii) ECMA script escape sequences, including named sets, octal, hexadecimal and Unicode sets; and (iv) character-encoding switches.

[0065] Preferably, decoder 250 takes normalized input from normalizer 240. In accordance with a preferred embodiment of the present invention, decoder 250 is implemented as a finite-state machine. The FSM for decoder 250 terminates when it reaches a state that produces a decoded character. If decoder 250 fails to decode a sequence, then each character is processed by tokenizer 210 individually, and not as part of the sequence. Preferably, a plurality of decoders 250 can be pipelined to enable decoding of text that is encoded by one escape scheme over another, such as text encoded with a URL scheme and then encoded with ECMA script scheme inside of JavaScript strings.

[0066] Tokenizer 210 and normalizer 240 are generic modules that can be adapted to process any content language, by providing a description of the content language within a rule file. Preferably, the rule file describes text characters used within the content language, and the composition of constructs of the content language, referred to as tokens. Tokens may include inter alia, an IDENT token for the name of a variable or function, various punctuation

tokens, and tokens for keywords such as NEW, DELETE, FOR and IF. A sample rule file for JavaScript is provided in Appendix A, and is described hereinbelow.

[0067] In accordance with a preferred embodiment of the present invention, parser 220 controls the process of scanning incoming content. Preferably, parser 220 invokes tokenizer 210, giving it a callback function to call when a token is ready. Tokenizer 210 uses the callback function to pass parser 220 the tokens it needs to parse the incoming content. Preferably, parser 220 uses a parse tree data structure to represent scanned content. A parse tree contains a node for each token identified while parsing, and uses parsing rules to identify groups of tokens as a single pattern. Examples of parsing rules appear in Appendix A, and are described hereinbelow.

[0068] Preferably, the parse tree generated by parser 220 is dynamically built using a shift-and-reduce algorithm. Successive tokens provided to parser 220 by tokenizer 210 are positioned as siblings. When parser 220 discovers that a parsing rule identifies a group of siblings as a single pattern, the siblings are reduced to a single parent node by positioning a new parent node, which represents the pattern, in their place, and moving them down one generation under the new parent node.

[0069] Preferably, within the parse tree, each node contains data indicating inter alia an ID number, the token or rule that the node represents, a character string name as a value for the node, and a numerical list of attributes. For example, if the node represents an IDENT token for the name of a variable, then the value of the node is the variable name; and if the node represents a rule regarding a pattern for a function signature, then the value of the node is the function name.

[0070] In addition, whenever a parsing rule is used to recognize a pattern, information about the pattern may be stored within an internal symbol table, for later use.

[0071] In a preferred embodiment of the present invention, parsing rules are implemented as finite-state machines. These FSMs preferably return an indicator for (i) an exact match, (ii) an indicator to continue with another sibling node, or (iii) an indicator of a mis-match that serves as an exit.

[0072] More generally, parsing rules may be implemented using a hybrid mix of matching algorithms. Thus, it may use a deterministic finite automaton (DFA) for quick identification of rule candidates, and a non-deterministic finite automaton (NFA) engine for exact evaluation of the candidate rules.

[0073] DFA and NFA are well known in the art of compilers, as finite-state machine engines for pattern matching. Reference is now made to FIG. 4A, which is an example of an NFA for the pattern $1001^* \wedge [1002 \mid 1003 \mid 1004]^+$; i.e., a pattern of tokens with zero or more occurrences of 1001 followed by one or more occurrences of any of the three tokens 1002, 1003, 1004. The NFA is a directed graph with nodes and directed edges therebetween. The edges are labeled with token identifiers, and with a special symbol “epsilon.” Edges marked with token identifiers can only be traversed if the current token being processed matches the token for the edge. Edges marked with the symbol “epsilon” serve as pass-through nodes, and can be traversed at will, without reference to a token. The NFA attempts to find a path from a starting node 39 to a finishing node 40, via the directed edges, as successive tokens from an input sequence are processed. The path should be maximal in the sense that there is no edge to traverse for the next token in the input sequence. Searching for such a maximal path is often referred to in the art as a “greedy” algorithm.

[0074] For example, if the sequence of tokens 1001 1002 1003 1004 1001 is input, then the NFA processes the four tokens 1001 1002 1003 1004 and proceeds through the path with successive nodes 39, 3, 5, 6, 4, 17, 19, 20, 23, 24, 25, 28, 29, 30, 31, 32, 35, 38, 29, 36, 37, 38, 18 and 40. The token 1001 is matched at node 5, the token 1002 is matched at node 23, the token 1003 is matched at node 32 and the token 1004 is matched at node 36. However, from node 36 there is no sequence of edges that can match the next token 1001, and thus the NFA terminates successfully with the pattern 1001 1002 1003 1004.

[0075] In distinction, if the sequence of tokens 1001 1001 1001 is input, then the NFA processes the three 1001 tokens and proceeds through the path with successive nodes 39, 3, 5, 6, 5, 6, 5 and 6, from which point it fails to reach finishing node 40 for lack of an appropriate token to pass through any of nodes 21, 23 and 26.

[0076] It is noted that some of the nodes in FIG. 4A, such as nodes 3, 6, 19, 28 and 29, have more than one permissible outgoing edge labeled “epsilon.” The property of having more than one choice of edge to traverse at a given stage of processing, is what characterizes finite automata as being non-deterministic. At such nodes the NFA may have to back track and try more than one path in order to find a match. Thus at node 29, the NFA may try to follow a path through node 30 and, if unsuccessful, then back track to node 29 and follow a path through node 36. For this reason, although NFA are simpler to derive, they are often not as efficient as DFA.

[0077] Reference is now made to FIG. 4B, which is a DFA corresponding to the NFA of FIG. 4A. In contrast to the NFA of FIG. 4A, there are no nodes in the DFA labeled “epsilon,” and each node in the DFA has at most one permissible outgoing edge, for any given token. As such, there is no need for the DFA to ever back track. All of the nodes with double circles around them are finishing nodes. If the sequence of tokens 1001 1002 1003 1004 1001 is input, then the DFA processes the tokens 1001 1002 1003 1004 and proceeds through the path with successive nodes 1, 2, 3, 8 and 9. There is no outgoing edge at node 9 corresponding to the next token 1001 in the input sequence. As such, the DFA terminates successfully with the pattern 1001 1002 1003 1004.

[0078] Generation of a DFA equivalent to a given NFA is well known in the art of compilers, and generally uses algorithms referred to as “subset construction” and “DFA minimization.” In accordance with a preferred embodiment of the present invention, parser rules, and also analyzer rules described hereinbelow, are stored as an NFA engine, a DFA engine, or another finite-state machine engine. Preferably, the finite-state machine engine for a rule is generated by a rule compiler, which receives as input a semantic description of the rule such as the rule descriptions shown in Appendix A, formulated perhaps by a software engineer, and generates as output an appropriate finite-state machine engine.

[0079] In addition to a pattern, a parser rule optionally includes one or more actions to be performed if an exact pattern match is discovered. Actions that can be performed include inter alia creating a new node in the parse tree, as described hereinabove with respect to the shift and reduce algorithm; setting internal variables; invoking a sub-scanner 270, as

described hereinbelow; and searching the parse tree for nodes satisfying specific conditions. By default, when the pattern within a parser rule is matched, parser 220 automatically performs a reduce operation by creating a new node and moving token nodes underneath the new node. A rule may be assigned a NoCreate attribute, in which case the default is changed to not performing the reduction operation upon a match, unless an explicit addnode command is specified in an action for the rule.

[0080] Sub-scanner 270 is another ARB scanner, similar to scanner 200 illustrated in FIG. 2 but for a different type of content. Preferably, sub-scanner 270 is used to scan a subsection of input being processed by scanner 200. Thus, if an HTML scanner encounters a script element that contains JavaScript code, then there will be a rule in the HTML scanner whose action includes invoking a JavaScript scanner. In turn, the JavaScript scanner may invoke a URI scanner. Use of sub-scanner 270 is particularly efficient for scanning content of one type that contains content of another type embedded therein.

[0081] Preferably, immediately after parser 220 performs a reduce operation, it calls analyzer 230 to check for exploits. Analyzer 230 searches for specific patterns of content that indicate an exploit.

[0082] Preferably, parser 220 passes to analyzer 230 a newly-created parsing node. Analyzer 230 uses a set of analyzer rules to perform its analysis. An analyzer rule specifies a generic syntax pattern in the node's children that indicates a potential exploit. An analyzer rule optionally also includes one or more actions to be performed when the pattern of the rule is matched. In addition, an analyzer rule optionally includes a description of nodes for which the analyzer rule should be examined. Such a description enables analyzer 230 to skip nodes that are not to be analyzed. Preferably, rules are provided to analyzer 230 for each known exploit. Examples of analyzer rules appear in Appendix A, and are described hereinbelow.

[0083] As described hereinabove with respect to parser rules, analyzer rules are also preferably represented by finite-state machines such as NFAs and DFAs.

[0084] Preferably, the nodes of the parse tree also include data for analyzer rules that are matched. Specifically, if analyzer 230 discovers that one or more analyzer rules are matched

at a specific parsing tree node, then the matched rules are added to a list of matched rules stored within the node.

[0085] An advantage of the present invention is that both parser 220 and analyzer 230 use a common ARB regular expression syntax. As such, a common pattern matching engine 260 performs pattern matching for both parser 220 and analyzer 230. In accordance with a preferred embodiment of the present invention, pattern matching engine 260 accepts as input (i) a list of ARB regular expression elements describing a pattern of interest; and (ii) a list of nodes from the parse tree to be matched against the pattern of interest. Preferably, pattern matching engine 260 returns as output (i) a Boolean flag indicating whether or not a pattern is matched; and (ii) if the pattern is matched, positional variables that match grouped portions of the pattern. For example, if a pattern “(IDENT) EQUALS NUMBER” is matched, then \$1 is preferably set to a reference to the nodes involved in the IDENT token. That is, if a matched pattern is “(1 2 3) 4 5”, then \$1 refers to the nodes 1, 2 and 3 as a single group.

[0086] Preferably, the ARB regular expression that is input to pattern matching engine 260 is pre-processed in the form of a state machine for the pattern. Reference is now made to FIG. 5, which is an illustration of a simple finite state machine, used in accordance with a preferred embodiment of the present invention, for a pattern,

(IDENT <val==”foo” & match(*):Rule1> | List <val==”bar”>) EQUALS NUMBER

Specifically, the pattern of interest specifies either an IDENT token with value “foo” and that matches Rule1, or a List with value “bar”, followed by an EQUALS token and a NUMBER token.

[0087] Reference is now made to Appendix A, which is a source listing of an ARB rule file for the JavaScript language, in accordance with a preferred embodiment of the present invention. The listing in Appendix A is divided into six main sections, as follows: (i) vchars, (ii) tokens, (iii) token_pairs, (iv) attribs, (v) parser_rules and (vi) analyzer_rules.

[0088] The vchars section includes entries for virtual characters. Each such entry preferably conforms to the syntax

```
vchar vchar-name [action=string] (char | hex-num)
{
  vchar-pattern*
```

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

}

For example, the entry

```
vchar nl 0x0d
{
  [0x0d]+;
  [0x0a]+
}
```

converts a sequence of one or more CRs (carriage-returns) and a sequence of one or more LFs (line-feeds) to a newline meta-character.

[0089] The `vchars` section also includes entries for aliases, which are names for special virtual characters. Each such entry preferably conforms to the syntax

```
vchar_alias vchar-name
{
  hex-num
}
```

For example, the entry

```
Vchar_alias underscore
{
  0x5F;
}
```

identifies the hexadecimal number 0x5F with the name “underscore”.

[0090] The `tokens` section includes entries for language tokens for a scanner language; namely, JavaScript for Appendix A. Each such entry preferably conforms to the syntax `token-entry*` (cdata);

For example, the entry

```
LBRACE “[!left_curly_bracket!]” punct;
```

defines identifies a punctuation token, LBRACE, as a “left_curly_bracket”, which is an alias for 0x7B as defined in the previous `vchars` section. Note that aliases are preferably surrounded by exclamation points.

[0091] A CDATA token, for identifying strings or commented text, preferably conforms to the syntax

```
“start” “end” [“escape-pattern”] “skip-pattern”;
```

For example, the entry

DOUBLE_QUOTE DOUBLE_QUOTE “[!backslash!][!double_quote]?”

“^[!backslash!][!double_quote!]+”;

identifies a string as beginning and ending with a DOUBLE-QUOTE token, as previously defined, with an escape pattern that has a “backslash” followed by zero or one “double_quote”, and a skip pattern that has one or more characters other than “backslash” and “double_quote”.

[0092] The token_pairs section defines tokens that can validly appear in juxtaposition, and tokens that cannot validly appear in juxtaposition, in conformance with the language rules. Generally, when the tokenizer encounters an invalid juxtaposition, it inserts a virtual semi-colon. An entry for a token-pair preferably conforms to the syntax

```
{valid | invalid} [( token-ID | token-ID)* ]
[( token-ID | token-ID)* ];
```

For example, the entry

```
invalid IF (ELSE | FOR | WHILE | DOT);
```

indicates that an IF token cannot validly be followed by an ELSE, FOR, WHILE or DOT token. Thus, if an IF token followed by an ELSE, FOR, WHILE, or DOT token is encountered in the input, tokenizer 210 will insert a virtual delimiter character between them.

[0093] The parser-rules section has entries defining rules for the parser. Such entries preferably conform to the syntax

```
rule rule-name [nonode] [noanalyze] [nomatch]
{
    [patterns
    {
        ID-pattern*;
    }]
    [actions
    {
        action*;
    }]
}
```

[0094] A pattern is a regular expression of IDs, preferably conforming to the syntax

ID₁-expr ID₂-expr ... ID_n-expr

Preferably, ID-expr is one of the following:

- ID

- (ID [ID]*)
- ID <val==val>
- ID <id==rule-ID>
- ID <match(n) : rule-ID>
- ID <match(*) : rule-ID>
- ID <match(m,n) : rule-ID>

The modifiers ‘*’, ‘+’, ‘?’, ‘{m}’ and ‘{m,n}’ are used conventionally as follows:

- ‘*’ zero or more occurrences
- ‘+’ one or more occurrences
- ‘?’ zero or one occurrence
- ‘{m}’ exactly m occurrences
- ‘{m,n}’ between m and n occurrences, inclusive

For example, the pattern in the rule for FuncSig

(FUNCTION) (IDENT?) (List)

describes a keyword “function”, followed by zero or one IDENT token,, and followed by a “List”. In turn, the pattern in the rule for List

(LPAREN) ((Expr) (COMMA Expr)*)? (RPAREN)

describes a LPAREN token and a RPAREN token surrounding a list of zero or more Expr’s separated by COMMA tokens. In turn, the pattern in the rule for Expr

([ExprDelimTokens ExprLdelimTokens ExprLdelimRules]?
([[^] ExprDelimTokens ExprLdelimTokens ExprLdelimRules ExprExcludeRules
ExprRdelimTokens]+ [ExprDelimTokens ExprRdelimTokens]) | ([ExprStmntRules]));

describes a general definition of what qualifies as an expression, involving delimiter tokens and other rules.

[0095] An action prescribes an action to perform when a pattern is matched. For example, the action in the rule for FuncSig

```
this.val=$(2).val;
@("FUNCNAME").val=$(2).val;
```

assigns a value to FuncSig, which is the value of the second parameter in the pattern for FuncSig; namely, the value of the IDENT token. In addition, the action assigns this same value to an entry in a symbol table called “FUNCNAME”, as described hereinbelow. It may thus be appreciated that certain rules have values associated therewith, which are assigned by the parser as it processes the tokens.

[0096] The symbol table mentioned hereinabove is an internal table, for rules to store and access variables.

[0097] The analyzer-rules section has entries defining rules for the parser. Such entries preferably conform to the syntax

```
rule rule-name [nonode] [noanalyze] [nomatch]
{
    [nodes
    {
        ID-pattern;
    }]
    [patterns
    {
        ID-pattern*;
    }]
    [actions
    {
        action*;
    }]
}
```

Patterns and actions for analyzer rules are similar to patterns and actions for parser rules.

[0098] Referring back to the example above, the pattern

(IDENT) ASSIGNMENT IDENT <val=="screen"> DOT IDENT <val=="width">

within the rule for ScrWidAssign describes a five-token pattern; namely, (i) an IDENT token, followed by (ii) an ASSIGNMENT token, followed by (iii) an IDENT token that has a value equal to “screen”, followed by (iv) a DOT token, and followed by (v) an IDENT token that has a value equal to “width”. Preferably, the value of an IDENT (i.e., an identifier) is its name; thus such a pattern indicates use of a member reference “screen.width” within an assignment statement, and corresponds to the example exploit listed above in the discussion of FIG. 1. For example, it corresponds to an assignment of the form

w = screen.width

[0099] The action

@(\$ (1).val).attr += ATTR_SCRWID

within the ScrWidAssign rule assigns the attribute ATTR_SCRWID to the symbol table entry whose name is the value of the IDENT token on the left side of the pattern. Specifically, for the example above the attribute ATTR_SCRWID is assigned to the symbol table entry for w.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068**[00100]** Similarly, the pattern

```
LPAREN Expr COMMA Expr COMMA Expr <attr?=ATTR_SCRWID> COMMA
  Expr <attr?=ATTR_SCRHGT>;
```

within the rule for ScrWidHgtList identifies an eight-token pattern; namely, (i) an LPAREN token (i.e., a left parenthesis), followed by (ii) an expression Expr, followed by (iii) a COMMA token (i.e., a comma), followed by (iv) another Expr, followed by (v) another COMMA token, followed by (vi) an Expr with attribute equal to ATTR_SCRWID, followed by (vii) another COMMA token, and followed by (viii) an Expr with attribute equal to ATTR_SCRHGT). Such a pattern includes inter alia any pattern

```
op.show(0,0, w, h, document.body)
```

for which w is a variable with attribute ATTR_SCRWID and h is a variable with attribute ATTR_SCRHGT.

[00101] Preferably, attributes are passed through assignments. For example, if an assignment is encountered of the form

```
a = w
```

where w is a variable with attribute ATTR_SCRWID, then the attribute ATTR_SCRWID is assigned to the symbol table entry for a. Similarly, if an assignment of the form

```
w = 10
```

is encountered, then the symbol table entry for w will no longer have the attribute ATTR_SCRWID. Thus it may be appreciated that analyzer rules are able to distinguish successfully between the malicious and non-malicious versions of code in the example above.

[00102] Similarly, the pattern

```
IDENT <@(val).attr?=ATTR_WINDOW>
  DOT FuncCall <val=="show" & matches(1):RULE(ScrWidHgtList)>;
```

in the rule for WndShowScrnWidHgt1 corresponds to the command

```
op.show(0,0, w, h, document.body)
```

in the example exploit above; and the pattern

```
(IDENT) ASSIGNMENT IDENT <@(val).attr?=ATTR_WINDOW>
  DOT FuncCall <val=="createPopup"> $;
```

in the rule for CreatePopup1 corresponds to the command

op=window.createPopup().

The action for the rule for Begin assigns attribute ATTR_WINDOW to the symbol table entry to “window”, and thus the action for CreatePopup1 assigns this attribute ATTR_WINDOW to the symbol table value for op. In turn, the rule for WndShowScrnWidHight1 recognizes that op satisfies the condition <@(val).attr?=ATTR_WINDOW.

[00103] It may thus be appreciated that exploits are generally described in terms of composite pattern matches, involving logical combinations of more than one pattern.

[00104] Node patterns within analyzer rules preferably specify nodes for which an analyzer rule should be evaluated. Node patterns serve to eliminate unnecessary analyses.

[00105] Referring back to FIG. 2, when parser 220 finds a pattern match for a specific parser rule, it preferably creates a node in the parser tree, and places the matching nodes underneath the newly created node. Preferably, parser 220 assigns the name of the specific rule to the name of the new node. However, if the rule has a “nonode” attribute, then such new node is not created.

[00106] After performing the actions associated with the specific rule, parser 220 preferably calls analyzer 230, and passes it the newly-created parser node of the parser tree. However, if the rule has a “noanalyzer” attribute, then analyzer 230 is not called.

[00107] When analyzer 230 finds a pattern match for a specific analyzer rule, it preferably adds the matched rule to the parser tree. However, if the rule has a “nomatch” attribute, then the matched rule is not added to the parser tree.

[00108] Reference is now made to FIG. 6, which is a simplified flowchart of operation of a parser for a specific content language, such as parser 220 (FIG. 2), within an ARB content scanner, such as content scanner 130 (FIG. 1), in accordance with a preferred embodiment of the present invention. Prior to beginning the flowchart in FIG. 6, it is assumed that the parser has initialized a parse tree with a root node. At step 600, the parser calls a tokenizer, such as tokenizer 210, to retrieve a next token from an incoming byte stream. At step 610 the parser adds the token retrieved by the tokenizer as a new node to a parse tree. Preferably, new nodes are added as siblings until a match with a parser rule is discovered.

[00109] Nodes within the parse tree are preferably named; i.e., they have an associated value that corresponds to a name for the node. Preferably, new nodes added as siblings are named according to the name of the token they represent.

[00110] At step 620 the parser checks whether or not a pattern is matched, based on parser rules within a rule file for the specific content language. If not, then control returns to step 600, for processing the next token. If a match with a parser rule is discovered at step 620, then at step 630 the parser checks whether or not the matched parser rule has a “nonode” attribute. If so, then control returns to step 600. If the matched parser rule does not have a “nonode” attribute, then at step 640 the parser performs the matched parser rule’s action. Such action can include inter alia creation of a new node, naming the new node according to the matched parser rule, and placing the matching node underneath the new node, as indicated at step 640. Thus it may be appreciated that nodes within the parse tree have names that correspond either to names of tokens, or names of parser rules.

[00111] At step 650 the parser checks whether or not the matched parser rules has a “noanalyze” attribute. If so, then control returns to step 620. If the matched parser rules does not have a “noanalyze” attribute, then at step 660 the parser calls an analyzer, such as analyzer 230, to determine if a potential exploit is present within the current parse tree. It may thus be appreciated that the analyzer is called repeatedly, while the parse tree is being dynamically built up.

[00112] After checking the analyzer rules, the analyzer returns its diagnostics to the parser. At step 670 the parser checks whether or not the analyzer found a match for an analyzer rule. If not, then control returns to step 600. If the analyzer did find a match, then at step 680 the parser performs the matched analyzer rule’s action. Such action can include inter alia recording the analyzer rule as data associated with the current node in the parse tree; namely, the parent node that was created at step 640, as indicated at step 680.

[00113] In accordance with a preferred embodiment of the present invention, binary class instances of ARB scanners are packaged serially, for transmission to and installation at a client site. Reference is now made to FIG. 7, which is a simplified block diagram of a system for serializing binary instances of ARB content scanners, transmitting them to a client site,

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

and regenerating them back into binary instances at the client site. The workflow in FIG. 7 begins with a set of rule files for one or more content languages. Preferably, the rule files are generated by one or more people who are familiar with the content languages.

[00114] A rule-to-XML convertor 710 converts rule files from ARB syntax into XML documents, for internal use. Thereafter a builder module 720 is invoked. Preferably, builder module 720 generates a serialized rule data file, referred to herein as an archive file.

[00115] In turn, ARB scanner factory module 730 is responsible for producing an ARB scanner on demand. Preferably, an ARB scanner factory module has a public interface as follows:

```
class arbScannerFactory
{
    INT32 createScanner(const std::string& mimeType, arbScanner** scanner);
    INT32 retireScanner(arbScanner *scanner, INT32& factoryStillActive);
    Bool hasScannerType(const std::string& mimeType);
}
```

ARB scanner factory module 730 is also responsible for pooling ARB scanners for later re-use.

[00116] ARB scanner factory module 730 instantiates a scanner repository 740. Repository 740 produces a single instance of each ARB scanner defined in the archive file. Preferably, each instance of an ARB scanner is able to initialize itself and populate itself with the requisite data.

[00117] Reference is now made to FIG. 8, which illustrates a representative hierarchy of objects created by builder module 720, in accordance with a preferred embodiment of the present invention. Shown in FIG. 8 are four types of content scanners: a scanner for HTML content, a scanner for JavaScript content, and a scanner for URI content. An advantage of the present invention is the ability to generate such a multitude of content scanners within a unified framework.

[00118] After ARB scanner factory module 730 is produced, builder module 720 calls a `serialize()` function. As such, the `serialize()` function called by builder module 720 causes all relevant classes to serialize themselves to the archive file recursively. Thereafter the archive file is sent to a client site.

[00119] After receiving the archive file, the client deserializes the archive file, and creates a global singleton object encapsulating an ARB scanner factory instance 750. The singleton is initialized by passing it a path to the archive file.

[00120] When the client downloads content from the Internet it preferably creates a pool of thread objects. Each thread object stores its ARB scanner factory instance 750 as member data. Whenever a thread object has content to parse, it requests an appropriate ARB scanner 760 from its ARB scanner factory object 750. Then, using the ARB scanner interface, the thread passes content and calls the requisite API functions to scan and process the content. Preferably, when the thread finishes scanning the content, it returns the ARB scanner instance 760 to its ARB scanner factory 750, to enable pooling to ARB scanner for later re-use.

[00121] It may be appreciated by those skilled in the art that use of archive files and scanner factories enables auto-updates of scanners whenever new versions of parser and analyzer rules are generated.

[00122] In reading the above description, persons skilled in the art will realize that there are many apparent variations that can be applied to the methods and systems described. Thus, although FIG. 6 describes a method in which a complete diagnostic of all match analyzer rules is produced, in an alternative embodiment the method may stop as soon as a first analyzer rule is matched. The parser would produce an incomplete diagnostic, but enough of a diagnostic to determine that the scanned content contains a potential exploit.

[00123] In addition to script and text files, the present invention is also applicable to parse and analyze binary content and EXE files. Tokens can be defined for binary content. Unlike tokens for text files that are generally delimited by punctuation characters, tokens for binary content generally have different characteristics.

[00124] The present invention can be embodied within a network gateway, as described hereinabove, or alternatively within a client computer as a desktop application. Reference is now made to FIG. 9, which is a simplified block diagram of a desktop computer implementation of an ARB content scanner, in accordance with a preferred embodiment of the present invention. Shown in FIG. 9 is a desktop computer 900 including a network

interface 910, which receives TCP/IP content from the Internet, including inter alia web pages via HTTP and secure HTTP, files via FTP, and e-mail via SMTP and POP3.

[00125] Desktop computer 900 preferably includes a network traffic probe 920, which generally passes incoming network traffic to its destination, be it a browser, e-mail client or other Internet application. However, in accordance with a preferred embodiment of the present invention, network traffic probe selectively diverts incoming network traffic to ARB scanner 930. ARB scanner 930 scans and analyzes content to detect the presence of potential exploits. To this end, desktop computer 900 preferably maintains a database 940 of coded exploit rules in the form of deterministic or non-deterministic finite automata, which perform pattern matches appropriate to exploits under consideration. If ARB scanner 930 does not detect a match with a potential exploit, then the content is routed to its destination.

Otherwise, if ARB scanner 930 detects the presence of potential exploits, then the suspicious content is passed to content blocked 950, which removes or inoculates such content.

[00126] In order to keep exploit rule database 940 current, desktop computer 800 preferably includes a rules update manager 960, which periodically receives modified rules and new rules over the Internet, and updates database 940 accordingly.

[00127] Reference is now made to FIG. 10, which is a simplified block diagram of a rule server that updates rule databases for the desktop computer 900 of FIG. 9, in accordance with a preferred embodiment of the present invention. Shown in FIG. 10 is a rules update server computer 1010, which serves as a source for current exploit rules. Typically, when a rule is added for a new exploit, a rules compiler 1020 processes a semantic characterization of the exploit to produce an appropriate coded rule in the form of a deterministic or non-deterministic finite automaton. In turn, the newly coded rule is transmitted to desktop computer 900, for incorporation into its local database 940.

[00128] It may be appreciated that the mechanism of FIG. 10 enables rules update server 1010 to propagate the most up-to-date rules to a plurality of desktop computers, and enables rule engineers to continually build up a database of exploit rules.

[00129] The ability to distribute ARB scanners among desktop computers residing at the periphery of a network is of advantage to the entire network. Scanning results for mobile

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

code, i.e., security profiles, are centrally cached at a network server or gateway, such as rules update server 1010, indexed according to IDs, such as a hash values, for the mobile code; and made available to other desktop computers within the network. Use of IDs for caching security profiles is described in applicant's US Patent No. 6804780, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables."

[00130] In accordance with a preferred embodiment of the present invention, desktop computer 900 includes a local cache for saving security profiles. The local cache communicates bi-directionally with the central network cache. Security profiles generated at desktop computer 900 are communicated to the central network cache, in order to update the central network cache; and conversely desktop computer 900 periodically updates itself from the central network cache, so as to maintain up-to-date security profiles.

[00131] When ARB scanner 930 receives content to scan, it first checks if a security profile for the content is already available in cache. If so, then ARB scanner does not need to scan the content, and can use the security profile previously derived by itself or by an ARB scanner from another desktop computer. Thus it may be appreciated that desktop computers mutually benefit one another from the security profiles that they generate and share among themselves.

[00132] Reference is now made to FIG. 11, which is a simplified block diagram of a network security system that takes advantage of distributed ARB scanners to populate a central security profile cache, in accordance with a preferred embodiment of the present invention. Shown in FIG. 11 are four desktop computers 1110 inter-connected within a network. Each desktop computer includes its own ARB scanner 1120 and local security profile cache 1130. When processing incoming content, each ARB scanner 1120 preferably derives an ID for the content, such as a hash value, and checks local cache 1130 to ascertain whether or not a security profile already exists corresponding to the ID. If so, then ARB scanner 1120 uses the cached security profile, and does not need to derive a security profile for the content. If not, then ARB scanner 1120 derives a security profile for the content, and stores the content ID and security profile on local cache 1130.

[00133] Additionally, ARB scanner 1120 also transmits the content ID and security profile to a central security profile cache 1140 for storage. In this way, central security profile cache 1140 integrates security profile information from all of the desktop computers 1110. Periodically, each local security profile cache 1130 is updated based on information in central security profile cache 1140, so as to synchronize the local security profile caches. In this way, each local security profile cache 1130 within desktop computer 1110 benefits from the combined efforts of the other desktop computers.

[00134] It may be appreciated that the present invention applies beneficially to other types of distributed computers in addition to desktop computers, including inter alia mobile computers, wireless computers and cellular telephones.

[00135] Content scanned by ARB scanners may contain various elements assigned by a web server when the content is served to a client, such as HTML tags with date & time stamps. Such elements, if included when an ARB scanner derives an ID for the content, artificially distinguish between instances of the same content with different date & time stamps. In accordance with a preferred embodiment of the present invention, such elements are removed by an ARB scanner when deriving an ID for the content, so that the ID reflects the operational part of the content. The ID as derived by the present invention is thus invariant for multiple instances of the same mobile code that arrive at one or more ARB scanners at different times.

[00136] In applicant's US Patent Nos. 6167520 and 6480962, both entitled "System and Method for Protecting a Client during Runtime from Hostile Downloadables," there is described a desktop security system and method that operates by confining suspicious content to run within an isolated environment referred to as a "sand box." The sand box acts as a simulator in a "clean room" environment, and buffers suspicious operations from harming a computer system.

[00137] It may be appreciated that the sandbox invention and the present invention of desktop ARB scanning complement each other. Specifically, it is noted that the ARB scanner carries out a general behavioral analysis for content, which may be conditional upon specific data values. For example, an operating system command identified by the ARB scanner may

or may not be harmful, depending upon values of various system parameters at the time the command is evoked. Such a command may be a harmful command that modifies crucial system data, or may be a harmless command simply to retrieve the current time and display it.

[00138] On the other hand, sandbox analysis of content only determines the behavior of suspicious code under specific conditions; namely, the conditions at the time the suspicious code is run. Unlike the ARB analysis, the sandbox analysis cannot predict the behavior of the suspicious code under different sets of conditions. Thus it may be appreciated that the sandbox and ARB analyses add significant value to one another, and can be synergistically combined.

[00139] By combining the sandbox and ARB analyses, behavior that is conditionally suspicious is better treated, so as to avoid over-blocking. The ARB scanner is relaxed to be more flexible and allow conditionally suspicious behavior to pass, knowing that the sandbox analysis will catch such behavior, if it proves to be harmful, while the content is trying to execute. In turn, malicious behavior recognized by the sandbox analysis is recorded in the security profile for the content, thereby producing a security profile that more accurately diagnoses conditionally suspicious behavior.

[00140] Reference is now made to FIG. 12, which is a simplified block diagram of an integrated content scanner including a general behavioral scanner and a sandbox scanner, in accordance with a preferred embodiment of the present invention. As shown in FIG. 12, incoming content is received by ARB scanner 1210. ARB scanner 1210 derives an ID for the content and checks a local security profile cache 1220 to determine whether or not a security profile for the content already resides in local cache. If so, then ARB scanner 1210 does not need to derive the security profile, saving significant processing time. If not, then ARB 1210 scanner performs a general behavioral scan of the content, using an adaptive rule-based analysis. ARB analysis is generally carried out without executing the content being analyzed. Such analysis often identifies conditionally malicious code; i.e., code that is or is not malicious depending upon values of operational data that are determined at run-time. Without further information, such content is generally blocked unconditionally in order not to

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

compromise system security. However, such blocking of content with conditionally malicious code is a source of unwanted over-blocking.

[00141] In accordance with a preferred embodiment of the present invention, over-blocking of content with conditionally malicious code is mitigated by integrating ARB scanner 1210 with sandbox scanner 1230. Sandbox scanner analyzes content by executing the content within a protected environment, so that the content does not have access to critical system data including inter alia operating system data, file system data and network communication data. The analysis performed by sandbox scanner is specific to one set of values of operational data; namely, the values at the time the content is executed.

[00142] Whereas ARB scanner 1210 conducts a general behavioral analysis that identifies malicious code within content under general operating conditions, sandbox scanner 1230 conducts an analysis that is specific to one particular set of operating conditions. As a result, code that is identified as conditionally malicious by ARB scanner 1210 can be further analyzed by sandbox scanner 1230 to ascertain whether or not the code is malicious under a specific set of conditions. If sandbox scanner 1230 determines that the conditionally malicious code within the content is in fact malicious under the specific set of conditions, then preferably sandbox scanner 1230 modifies the security profile of the content to reflect the malicious behavior, thereby improving upon the security profile generated by ARB scanner 1210.

[00143] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made to the specific exemplary embodiments without departing from the broader spirit and scope of the invention as set forth in the appended claims. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A security system for scanning content within a computer, comprising:
 - a network interface, housed within a computer, for receiving content from the Internet on its destination to an Internet application running on the computer;
 - a database of rules corresponding to computer exploits, stored within the computer;
 - a rule-based content scanner that communicates with said database of rules, for scanning content to recognize the presence of potential exploits therewithin;
 - a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting content from its intended destination to said rule-based content scanner; and
 - a rule update manager that communicates with said database of rules, for updating said database of rules periodically to incorporate new rules that are made available.

2. The security system of claim 1 wherein said database of rules stores rules in the form of pattern-matching engines.

3. The security system of claim 2 wherein the pattern-matching engines are deterministic finite automata.

4. The security system of claim 2 wherein the pattern-matching engines are non-deterministic finite automata.

5. The security system of claim 1 further comprising a content blocker, operatively coupled to said rule-based content scanner, for preventing a potential exploit that was recognized by said rule-based content scanner from reaching its intended destination.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

6. The system of claim 1 wherein the content received from the Internet by said network interface is HTTP content.

7. The system of claim 1 wherein the content received from the Internet by said network interface is HTTPS content.

8. The system of claim 1 wherein the content received from the Internet by said network interface is FTP content

9. The system of claim 1 wherein the content received from the Internet by said network interface is SMTP content

10. The system of claim 1 wherein the content received from the Internet by said network interface is POP3 content

11. The system of claim 1 wherein the destination Internet application is a web browser.

12. The system of claim 1 wherein the destination Internet application is an e-mail client.

13. A method for scanning content within a computer, comprising:
receiving content from the Internet on its destination to an Internet application;
selectively diverting the received content from its intended destination;
scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of rules corresponding to computer exploits; and
updating the database of rules periodically to incorporate new rules that are made available.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

14. The method of claim 13 wherein said database of rules stores rules in the form of pattern-matching engines.

15. The method of claim 14 wherein the pattern-matching engines are deterministic finite automata.

16. The method of claim 14 wherein the pattern-matching engines are non-deterministic finite automata.

17. The method of claim 13 further comprising preventing a potential exploit that was recognized by said scanning from reaching its intended destination.

18. The method of claim 13 wherein the content received from the Internet by said network interface is HTTP content.

19. The method of claim 13 wherein the content received from the Internet by said network interface is HTTPS content.

20. The method of claim 13 wherein the content received from the Internet by said network interface is FTP content

21. The method of claim 13 wherein the content received from the Internet by said network interface is SMTP content

22. The method of claim 13 wherein the content received from the Internet by said network interface is POP3 content

23. The method of claim 13 wherein the destination Internet application is a web browser.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

24. The method of claim 13 wherein the destination Internet application is an e-mail client.

25. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving content from the Internet on its destination to an Internet application;

selectively diverting the received content from its intended destination;

scanning the selectively diverted content to recognize potential exploits therewithin, based on a database of rules corresponding to computer exploits; and

updating the database of rules periodically to incorporate new rules that are made available.

Express Mail Label No. EV 609 138 904 US

PATENT
43426.00068

ABSTRACT OF THE DISCLOSURE

A security system for scanning content within a computer, including a network interface, housed within a computer, for receiving content from the Internet on its destination to an Internet application running on the computer, a database of rules corresponding to computer exploits, stored within the computer, a rule-based content scanner that communicates with said database of rules, for scanning content to recognize the presence of potential exploits therewithin, a network traffic probe, operatively coupled to the network interface and to the rule-based content scanner, for selectively diverting content from its intended destination to the rule-based content scanner, and a rule update manager that communicates with said database of rules, for updating said database of rules periodically to incorporate new rules that are made available. A method and a computer readable storage medium are also described and claimed.