EXHIBIT E

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!][!dollarsign!]] [A-Za-z0-9[!underscore!][!dollarsign!]]*",

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

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:

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.

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 ~~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

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 ~~logical combinations of~~ patterns of types of tokens, tokens being program code constructs; 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.

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.

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*

(<A HREF=\f "Symbol">, or <IMG SRC=\f "Symbol"> 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

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.

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

By: */Eric L. Sophir, Reg. #48,499/*

Eric L. Sophir
Registration No. 48,499
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4706
(202) 737-0500

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:

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.

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

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.

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

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

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**, **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*

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 user 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.*"

"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 users 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.

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*

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.

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.

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

By: */Eric L. Sophir, Reg. #48,499/*

Eric L. Sophir
Registration No. 48,499
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4706
(202) 737-0500

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of:	
Moshe Rubin Moshe Matitya Artem Melnick Shlomo Touboul Alexander Yermakov Amit Shaked	Examiner: Jeffery L. Williams Art Unit: 2437
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]	*"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."*
Par. [0012]	*"This description language enable an engineer to describe exploits as logical combinations of patterns of tokens."*

Par. [0042]	*"Portions of code that are malicious are referred to as exploits."*
Par. [0044]	*"… a behavioral approach that analyses content based on its behavior instead of its binary structure."*
Par. [0055]	*"An ARB scanner system … is customized for a specific language through use of a set of language-specific rules."*
Par. [0056]	*"Moreover … security violations, referred to as exploits, are described using a generic syntax, which is also language-independent."*
Par. [0057]	*"… 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 …"*
Par. [0066]	*"Preferably, the rule file describes text characters used within the content language, and the composition of constructs of the content language …"*
Par. [0082]	*"An analyzer rule specifies a general syntax pattern … that indicates a potential exploit … rules are provided to analyzer 230 for each known exploit"*
Pars. [0097] – [00102]	Analyzer rule for the exploit indicated in Pars. [0042] and [0043]
Par. [00103]	*"… exploits are generally described in terms of composite pattern matches, involving logical combinations of more than one pattern."*
Pars. [00111] and [00112]	*"… 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 …"*
Par. [00113]	*"Preferably, the rule files are generated by one or more people who are familiar with the content languages."*
Par. [00122]	*"… the method may stop as soon as a first analyzer rule is matched … to determine that the scanned content contains a potential exploit."*
Par. [00125]	*"… a database 940 of coded exploit rules … which perform pattern matches appropriate to exploits …"*
Par. [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."*
Par. [00127]	*"… a rule server that updates rule databases for the desktop computer …"*
Par. [00128]	*"… 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."*
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/*

Eric L. Sophir
Registration No. 48,499
KING & SPALDING LLP
1700 Pennsylvania Ave., NW
Suite 200
Washington, DC 20006
(202) 737-0500

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:

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

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:

[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

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

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

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 ~~contract~~ 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

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,

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

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. ~~6804780~~ 6,804,780, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables."

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 [[1210]] 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

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.

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.

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

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.

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

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.

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

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.

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

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*

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.

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

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

Dawn-Marie Bey
Registration No. 44,442
KING & SPALDING LLP
1700 Pennsylvania Ave., NW
Suite 200
Washington, DC 20006
(202) 737-0500