Trials@uspto.gov
571-272-7822

Paper No. 10
Entered: January 31, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ESET, LLC and ESET spol s.r.o.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

Case IPR2017-01738
Patent 7,975,305 B2

Before JAMES B. ARPIN, PATRICK M. BOUCHER, and ZHENYU YANG, *Administrative Patent Judges*.

BOUCHER, *Administrative Patent Judge.*

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

ESET, LLC, and ESET spol s.r.o. (collectively, "Petitioner") filed a Petition (Paper 2, "Pet.") pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–25 of U.S. Patent No. 7,975,305 B2 ("the '305 patent"). Finjan, Inc. ("Patent Owner") filed a Preliminary Response (Paper 9, "Prelim. Resp."). Applying the standard set forth in 35 U.S.C.

§ 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we institute *inter partes* review of claims 1–25. The Board has not made a final determination of the patentability of any claim.

I. BACKGROUND

A. The '305 Patent

1. Disclosure

The '305 patent relates to network security, including scanning of mobile content for exploits through "behavioral analysis," in which incoming content is analyzed in terms of its programmatic behavior—"[a]s distinct from prior art approaches that search for byte patterns." Ex. 1001, col. 1, ll. 24–25, col. 1, ll. 64–67. "Exploits" are "[p]ortions of code that are malicious"; the '305 patent provides an example that uses JavaScript to create a window that fills an entire screen, leaving the user unable to access any underlying windows. *Id.* at col. 5, l. 65–col. 6, l. 3.

Figure 2 of the '305 patent is reproduced below.

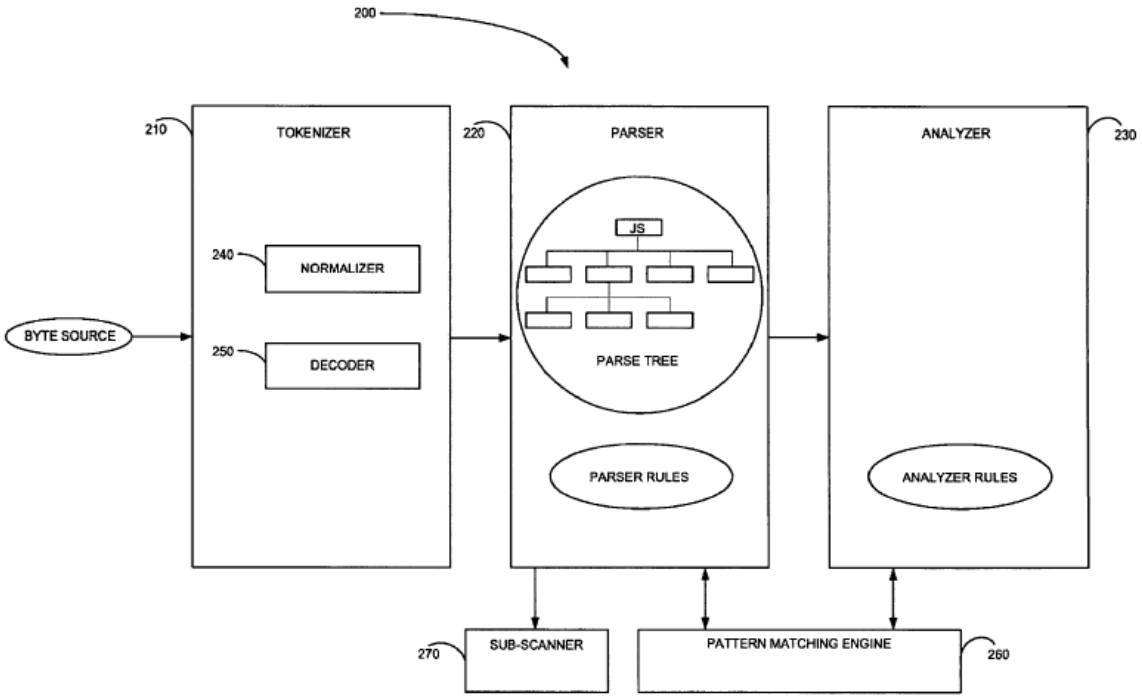

FIG. 2

Figure 2 provides a simplified block diagram of an adaptive rule-based content scanner system, which is "able to adapt itself dynamically to scan a specific type of content, such as inter alia JavaScript, VBScript, URI, URL and HTML." *Id.* at col. 6, ll. 14–17, col. 2, ll. 10–14. The '305 patent explains that the adaptive rule-based scanner of Figure 2 "is preferably designed as a generic architecture that is language-independent, and is customized for a specific language through use of a set of language-specific rules." *Id.* at col. 8, ll. 43–46. In addition, "security violations, referred to as exploits, are described using a generic syntax, which is also language-independent." *Id.* at col. 8, ll. 54–56.

Adaptive rule-based scanner 200 includes three main components: (1) tokenizer 210, which recognizes and identifies constructs (i.e., "tokens") within a byte source code; (2) parser 220, which controls the process of

scanning incoming content, such as with a parse tree data structure that represents the incoming content; and (3) analyzer 230, which checks for exploits by searching for specific patterns of content that indicate an exploit. *Id.* at col. 9, ll. 9–14, col. 10, ll. 45–55, col. 12, ll. 54–57. Sub-scanner 270 is another adaptive rule-based scanner used to scan a subsection of input being processed by scanner 200. *Id.* at col. 12, ll. 43–44. Pattern matching engine 260 performs pattern matching for both parser 220 and analyzer 230, such as by accepting an input list of regular-expression elements describing a pattern of interest and an input list of nodes from the parse tree to be matched against the pattern of interest, and outputting a Boolean flag indicating whether a pattern is matched. *Id.* at col. 13, ll. 13–29.

Figure 9 of the '408 patent is reproduced below.

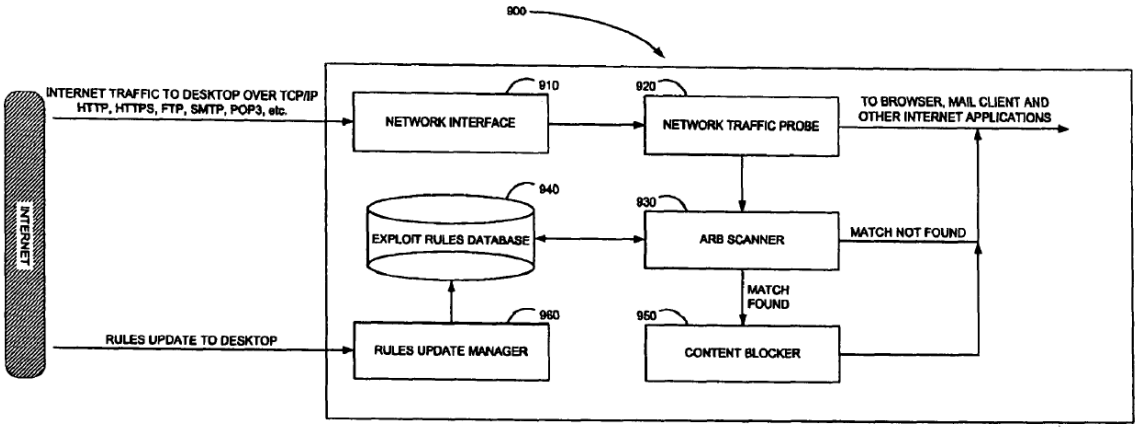

FIG. 9

Figure 9 is a simplified block diagram that illustrates a desktop-computer implementation of an adaptive rule-based content scanner. *Id.* at col. 19, ll. 26–30. Network interface 910 receives TCP/IP content from the Internet, and network traffic probe 920 passes incoming traffic to its destination, such as to a browser, email client, or other Internet application. *Id.* at col. 19, ll. 30–38. Network traffic probe 920 also "selectively diverts" incoming

network traffic to adaptive rule-based scanner 930, which scans and analyzes content to detect the presence of exploits. *Id.* at col. 19, ll. 38–42. In the context of Figure 1 (not reproduced here), the Specification of the '305 patent explains that a pre-scanner uses "conventional signature technology" to scan content, and can thereby "quickly determine if content is innocuous, but over-blocks on the safe side." *Id.* at col. 8, ll. 5–8. The pre-scanner, thus, is "useful for recognizing content that poses no security threat," with the adaptive rule-based scanner "perform[ing] much more intensive processing" for "further diagnosis" on content that is "potentially malicious." *Id.* at col. 8, ll. 9–21.

Database 940 is maintained with coded exploit rules "in the form of deterministic or non-deterministic finite automata, which perform pattern matches appropriate to exploits under consideration." *Id.* at col. 19, ll. 42–46. If adaptive rule-based scanner 930 does not detect a match with a potential exploit, the content is routed to its destination. *Id.* at col. 19, ll. 46–48. Conversely, if adaptive rule-based scanner detects the presence of potential exploits, the suspicious content is passed to content blocker 950, which removes or inoculates the content. *Id.* at col. 19, ll. 48–51. Rules update manager 960 periodically receives modified and new rules over the Internet, and updates database 940 to keep database 940 current. *Id.* at col. 19, ll. 52–55.

2. Illustrative Claim

Independent claim 1 of the '305 patent, reproduced below, recites a "security system for scanning content within a computer," and is illustrative of the claims at issue, with independent claims 13 and 25 respectively

reciting corresponding methods and computer-readable storage media. *See* Pet. 6–11 (tables provided by Petitioner illustrating correspondence of limitations).

> 1. 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.

Ex. 1001, col. 29, l. 44–col. 30, l. 47.

3. Prosecution History

Prosecution of the '305 patent focused extensively on whether the claims are anticipated by or rendered obvious over U.S. Patent No. 5,987,611 ("Freund"). During prosecution, the Office issued five Office Actions in which the Examiner rejected the claims, and to which Applicant responded. Ex. 1002, 121–134, 189–200, 239–247, 369–379, 445–451. In each Office Action, the Examiner addressed the disclosure of Freund and how it bears on the patentability of the claims. Ultimately, after certain amendments to the claims and after consideration of Applicant's responses regarding the disclosure of Freund, the Office allowed the application. *Id.* at 82–90. In allowing the application, the Examiner provided the following statement of reasons for allowance:

> The prior art fails to disclose the features, as found recited in combination with remaining claim limitations, of "*scanning, by the computer, the selectively diverted incoming content to recognize potential computer exploits therewithin, based on a database of parser and analyzer rules corresponding to computer exploits, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type*".

Id. at 88–89.

C. References

Petitioner relies on the following references.

Chandnani	US 7,636,945 B2	Dec. 22, 2009	Ex. 1013
Freund	US 5,987,611	Nov. 16, 1999	Ex. 1014

D. Asserted Grounds of Unpatentability

Petitioner challenges claims 1–25 over Chandnani alone and over Freund in combination with Chandnani. Pet. 18–62. There is an inconsistency in Petitioner's presentation in that it characterizes all of its challenges over Chandnani alone as anticipation challenges, *id.* at 18, but presents arguments that are clearly directed to obviousness challenges for claims 4–12 and 16–24, *id.* at 37–41. Because Petitioner's intent is sufficiently clear, we treat the Petition's challenges as follows.

Reference(s)	Basis	Claims
Chandnani	§ 102(e)	1–3, 13–15, and 25
Chandnani	§ 103(a)	4–12 and 16–24
Freund and Chandnani	§ 103(a)	1–25

E. Related Proceedings

The '305 patent is asserted by Patent Owner against Petitioner in Civil Action No. 3:17-cv-00183-CAB-BGS (S.D. Cal.). Pet. 1; Paper 3, 1.

The '305 patent is also the subject of Reexamination Control No. 90/013,660, which is currently on appeal to the Board. Pet. 1; Paper 3, 1.

II. ANALYSIS

A. Claim Construction

The Board interprets claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b) Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). Under the broadest reasonable interpretation standard, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary

skill in the art at the time of the invention. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). However, a "claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer and clearly set forth a definition of the disputed claim term in either the specification or prosecution history." *CCS Fitness, Inc. v. Brunswick Corp.Eyeglasses*, 288 F.3d 1359, 1366–67 (Fed. Cir. 2002). "Although an inventor is indeed free to define the specific terms used to describe his or her invention, this must be done with reasonable clarity, deliberateness, and precision." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). In the absence of such a special definition or other consideration, "limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Each of independent claims 1, 13, and 25 recites "a database of parser and analyzer rules corresponding to computer exploits, . . . 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." Ex. 1001, col. 29, ll. 49–56, col. 31, ll. 19–26, col. 32, ll. 28–35. The claim-construction issues raised by the parties involve only terms included within this recitation.

1. "database"

The parties agree that, for purposes of this proceeding, "database" means "a collection of interrelated data organized according to a database schema to serve one or more applications." Pet. 15; Prelim. Resp. 15. For purposes of this Decision, we adopt the parties' agreed construction.

2. "parser rules"

Petitioner proposes that "parser rules" be construed as "rules that identify a pattern of tokens," asserting that the Specification of the '305 patent "explains that 'parsing rules' are used to 'identify groups of tokens as a single pattern.'" Pet. 15 (quoting Ex. 1001, col. 10, ll. 53–55). Patent Owner counters that, "[i]n the context of the '305 Patent, the term 'parser rules' means ['']patterns of tokens that form syntactical constructs of program code' that 'identify groups of tokens as a single pattern.'" Prelim. Resp. 15 (quoting Ex. 1001, col. 2, ll. 22–24, col. 10, ll. 53–54).

We disagree with each party's proposed construction. The Specification of the '305 patent makes clear that what it "refer[s] to as parsing rules" are "patterns of tokens that form syntactical constructs of program code." Ex. 1001, col. 2, ll. 22–24. This is done with sufficient "clarity, deliberateness, and precision" for the Specification's statement to qualify as a definition of the term, which we adopt as the construction of "parser rules" for purposes of this Decision. *See Paulsen*, 30 F.3d at1480. Because Petitioner omits this definition from its proposed construction, we agree with Patent Owner that Petitioner's construction is "overbroad." *See* Prelim. Resp. 16.

Although each party incorporates the Specification's further language of "identify[ing] groups of tokens as a single pattern" into their proposed constructions, we disagree that such a requirement is properly included as part of the construction itself. The Specification provides that language in referring to use of the "parser rules" by a "parse tree," which is not recited in the claims. Ex. 1001, col. 10, ll. 53–54. Unlike Petitioner's proposed

construction, the cited portion of the Specification does not assert that the "parser rules" themselves "identify patterns of tokens"; rather, the "parser rules" are used by a "parse tree" for identifying such patterns. The claim language itself includes all that is necessary by reciting that "the parser . . . rules describe computer exploits as patterns of types of tokens," and this requirement need not be incorporated into the construction of "parser rules." *Id.* at col. 29, ll. 52–54.

Accordingly, for purposes of this Decision, we construe "parser rules" as "patterns of tokens that form syntactical constructs of program code."

3. "analyzer rules"

Petitioner proposes that "analyzer rules" be construed as "rules that provide 'a generic syntax pattern of tokens that indicates a potential exploit,'" asserting that the Specification describes "an analyzer rule specifies a generic syntax pattern in the node's children that indicates a potential exploit." Pet. 16 (quoting Ex. 1001, col. 12, ll. 60–62). Patent Owner responds that Petitioner's proposed construction "is overly narrow as it only applies to one embodiment of the invention described in the specification." Prelim. Resp. 17 (citing Ex. 1001, col. 8, ll. 53–56 ("Moreover, in accordance with a preferred embodiment of the present invention, security violations, referred to as exploits, are described using a generic syntax, which is also language-independent") (emphasis omitted)). Instead, Patent Owner proposes that "analyzer rules" be construed in accordance with the Specification's statement that "patterns of tokens that correspond to potential exploits [are] referred to as analyzer rules." Prelim. Resp. 17; Ex. 1001, col. 2, ll. 24–25.

We agree with Patent Owner. The Specification's more general statement that "analyzer rules" are "patterns of tokens that correspond to potential exploits" is made with sufficient "clarity, deliberateness, and precision" to qualify as a definition. *See Paulsen*, 30 F.3d at 1480. This more general statement is later qualified by the Specification for embodiments in which a general (language-independent) syntax is used to describe such patterns. To adopt Petitioner's proposed construction would improperly import a limitation from the Specification into the claims. *See Van Geuns*, 988 F.2d at 1184.

Accordingly, we construe "analyzer rules" as "patterns of tokens that correspond to potential exploits."

4. "function type"

Petitioner proposes that a "function type" token be construed as an "identity token that represents a function name." Pet. 16–17. Petitioner grounds its proposed construction by observing that "the '305 patent discloses three types of tokens (1) an identity token; (2) a punctuation token; and (3) a keyword token." Pet. 16 (citing Ex. 1001, col. 10, ll. 39–42). According to Petitioner, "the specification implies that a function token is a subset of the identity token." *Id.* at 16–17.

In contrast, while advocating that the term "function type" be accorded its plain and ordinary meaning, Patent Owner notes an example from the Specification of "a 'function type' token being a particular type of keyword token." Prelim. Resp. 19 (citing Ex. 1001, col. 15, ll. 19–22). In making their respective arguments, each party also refers to the following example from the Specification of the '305 patent:

> For example, if the node represents an IDENT token for the name of a variable, then the value of the node is the variable name; and if the node represents a rule regarding a pattern for a function signature, then the value of the node is the function name.

Ex. 1001, col. 11, ll. 1–5; *see* Pet. 16–17; Prelim. Resp. 19. Petitioner interprets this example as consistent with its proposed construction that a "function type" token is a form of identity token, while Patent Owner interprets this example as "explicitly distinguish[ing] function type tokens from 'an IDENT token for the name of a variable.'" Prelim. Resp. 19.

On the record before us, we conclude that Patent Owner presents the more persuasive argument, and that its argument is consistent with the prosecution history of the '305 patent. *See* Ex. 1002, 116 (identifying support in the Specification for "punctuation type," "identifier type," and "function type"). That is, we construe a "function type" token to be a form of keyword token that represents a function.

B. Challenges over Chandnani

1. Overview of Chandnani

Chandnani "relates to the detection of script language viruses," particularly polymorphic script language viruses, which copy themselves differently to change their signatures and make themselves appear different each time they spread. Ex. 1013, col. 1, ll. 15–18, col. 2, ll. 54–56. Figure 2 of Chandnani is reproduced below.

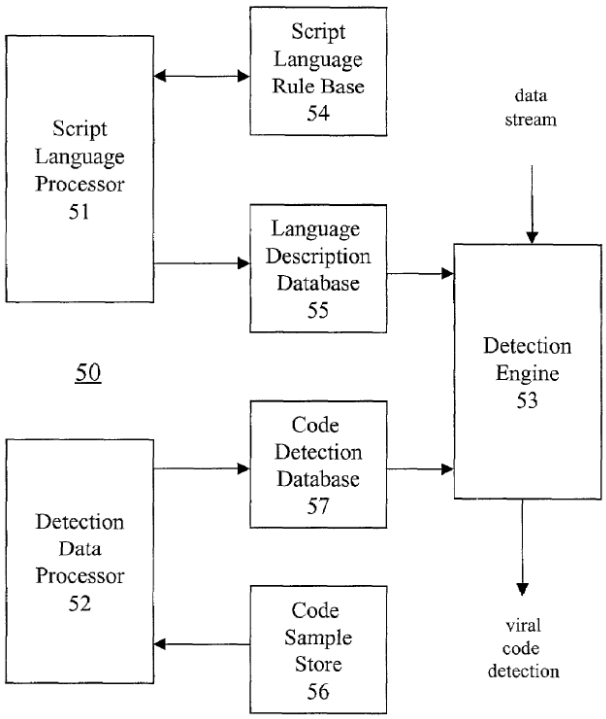

FIG. 2

Figure 2 provides a block diagram of a script language virus detection apparatus. *Id.* at col. 4, ll. 11–13. Language definition rules and language check rules are defined for respective target script languages and stored in rule base 54. *Id.* at col. 5, ll. 41–44. Such rules are processed by script language processor 51 to generate language description data for respective target script languages, stored in language description data module 55. *Id.* at col. 5, ll. 44–49. A data stream corresponding to a file to scan is tokenized by lexical analysis by feeding the data stream to a lexical analyzer in detection engine 53, which generates a stream of tokens. *Id.* at col. 8, ll. 4–7. The data stream is analyzed using the language check data to select the language definition data, and the selected language definition data and the data stream are supplied to the lexical analyzer, the process generating

tokens that correspond to a specific language construct. *Id.* at col. 8, ll. 7–17.

Chandnani describes a methodology in which "viral code detection data may include multiple layers of tests," with the tests "specified as a token pattern match methodology or a CRC signature check or a combination of token pattern match and CRC signature check methodologies." *Id.* at col. 7, ll. 1–5. Figure 7 of Chandnani is reproduced below.

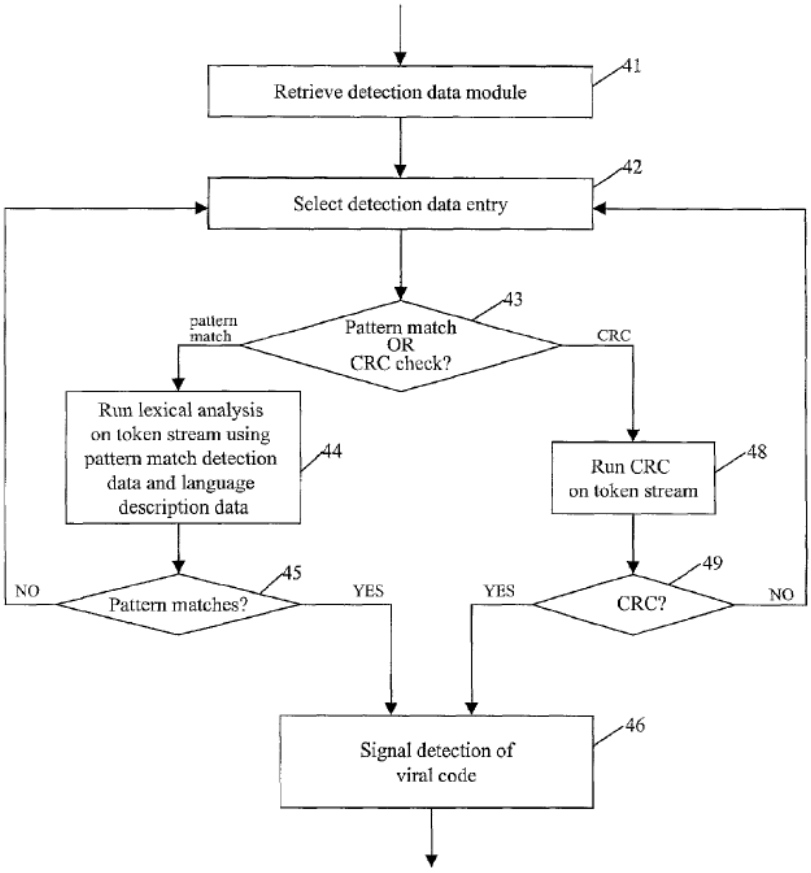

FIG. 7

Figure 7 is a "flow chart of a method of detecting a script language virus." *Id.* at col. 4, ll. 26–27.

After detection data stored in the detection database 57 are retrieved at block 41 and a detection data entry selected at block 42, "it is determined whether a selected check is a pattern match or virus or CRC signature check" at block 43. *Id.* at col. 8, ll. 44–50. If the check is a pattern match, "the token stream is analyzed lexically using the pattern match detection data and language description data" at block 44, with a determination made at block 45 whether there is a pattern match. *Id.* at col. 8, ll. 50–53. If the check is instead a CRC signature check, "the CRC is run on the token stream" at block 48, with a determination made at block 49 whether the CRC check succeeds. *Id.* at col. 8, ll. 53–56. If the pattern match or the CRC check is not successful, another detection data entry is selected at block 42. *Id.* at col. 8, ll. 56–59. Otherwise, if either check is successful, detection of viral code is signaled at block 46. *Id.* at col. 8, ll. 59–60.

2. Independent Claims 1, 13, and 25

We have reviewed Petitioner's analysis of independent claims 1, 13, and 25, and conclude that Petitioner demonstrates a reasonable likelihood of success that it would prevail with respect to its anticipation challenge of those claims. *See* Pet. 18–36. In particular, we agree that Petitioner makes a sufficient showing by identification of a "network interface . . . for receiving incoming content" as met by network 78 shown in Figure 1, by identification of a "rule-based content scanner . . . for scanning incoming content" as met by the lexical analysis described in connection with block 44, and by identification of a "rule update manager . . . for updating said database of

parser and analyzer rules" as met by the description of updating script language rule base 54 and code detection database 57 of Figure 2. *Id.* at 20–22, 32–34, 35–36. At this time, Patent Owner does not dispute these identifications in its Preliminary Response. We address other elements of the independent claims in further detail below.

a. "a database of parser and analyzer rules corresponding to computer exploits"

Each of independent claims 1, 13, and 25 recites "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." Ex. 1001 at col. 29, ll. 49–56, col. 31, ll. 19–26, col. 32, ll. 28–35. With respect to "parser rules," Petitioner draws a correspondence with Chandnani's "language definition rules," which Petitioner contends "define patterns in the data stream in terms of lexical constructs (tokens)." Pet. 23–25. Petitioner further contends that "Chandnani's 'language definition rules' – which are used to create language description data that is supplied to the detection engine – describe computer exploits as patterns of tokens, where the tokens are program code constructs." *Id.* at 23 (citing Ex. 1006 ¶¶ 49–51; Ex. 1013, col. 6, ll. 24–34, abst., Fig. 3, Fig. 7). Petitioner supports these contentions with testimony by Eugene H. Spafford, Ph.D. Ex. 1006 ¶¶ 49–51.

Patent Owner disputes this correspondence, arguing that the relations between constructs identified by Petitioner in Chandnani "are not akin to the

'parser rules' described and claimed in the '305 Patent, but rather to the 'token_pairs' rules." Prelim. Resp. 22. In addition, Patent Owner contends that Petitioner insufficiently addresses the claim requirement that the parser rules "correspond[] to computer exploits." *Id.* at 23.

At this stage, we are not persuaded by Patent Owner's arguments. At this time, Patent Owner has not offered expert testimony that controverts the opinions of Dr. Spafford, whose testimony we credit over the attorney argument provided by Patent Owner. *See In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974) (unsupported attorney argument in a brief cannot take the place of evidence). In addition, we find Petitioner's identification of Chandnani's "language definition rules" consistent with our preliminary construction of "parser rules" as "patterns of tokens that form syntactical constructs of program code."

With respect to "analyzer rules," Petitioner draws a correspondence with Chandnani's disclosure of pattern matching rules to identify potential viral code. Pet. 26 (citing Ex. 1013, col. 3, ll. 44–49, col. 8, ll. 43–60, col. 7, ll. 8–15, col. 9, ll. 24–34, Figs. 2, 3). Petitioner's position is supported by testimony by Dr. Spafford, and is sufficiently consistent with our preliminary construction of "analyzer rules" as "patterns of tokens that correspond to potential exploits." Ex. 1006 ¶¶ 54–56.

Petitioner also contends that Chandnani discloses "a database" of such parser and analyzer rules by identifying Script Language Rule Base 54 and

Code Detection Database 57. Pet. 27. Such identification is sufficient at this stage.[1]

On the record before us, Petitioner sufficiently identifies disclosure in Chandnani that corresponds to the recited "database of parser and analyzer rules corresponding to potential exploits."

b. "selectively diverting incoming content"

Each of independent claims 1, 13, and 25 recites a variant of a requirement for "selectively diverting" incoming content "from its intended destination." Ex. 1001, col. 29, ll. 63–66, col. 31, ll. 15–16, col. 32, ll. 25–26. Independent claim 1 specifically recites that the incoming content is "selectively divert[ed] . . . to said rule-based content scanner." *Id.* at col. 29, ll. 65–66. For these limitations, Petitioner refers to decision block 43 of Chandnani's Figure 7, reproduced above, which Petitioner contends "serves as a network traffic probe by selectively diverting only some content to the rule-based content scanner, depending upon the result of the CRC check."

[1] Patent Owner contends that these two databases are not "a database," as recited in the claims, i.e., that they are not "a single database." Prelim. Resp. 29. We are not persuaded, on the record before us, that "a single database" is required by the claims. *See KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1356 (Fed. Cir. 2000) ("Unless the claim is specific as to the number of elements, the article 'a' receives a singular interpretation only in rare circumstances when the patentee evinces a clear intent to so limit the article."). Moreover, a construction in which "a database" may encompass two databases is consistent with Figure 2 of the '305 patent, which illustrates "parser rules" and "analyzer rules" separately and distinctly associated with the "parser" and the "analyzer."

Pet. 35. Petitioner makes a sufficient showing at this stage with this identification.[2]

Patent Owner disputes this identification, arguing that "'decision box 43' never selectively diverts the data stream to box 44, where the 'pattern match' is performed because using a pattern match test is the default position in Chandnani." Prelim. Resp. 34. Patent Owner reasons that

> performing a pattern match test is the default in Chandnani's system, and such a test might only be avoided if the CRC check signals viral code, in which case it could be said that Chandnani diverts the data stream away from the pattern match test. But under no circumstance does this technique result in selectively diverting the data stream to the pattern match test.

Id. at 35. However, this argument is not persuasive because it implicitly relies on an interpretation of "selectively" incorporated from the Specification of the '305 patent. The Specification describes embodiments in which, based on the result of a signature check, incoming traffic is

[2] We are not persuaded by Petitioner's alternative argument that selective diversion is taught by Chandnani because its disclosure relates to "script language viruses." *See* Pet. 34. At best, Petitioner's expert asserts that "[t]hus, a person of skill in the art *could reasonably have interpreted* Chandnani as teaching diversion of only script languages to its rule-based scanner." Ex. 1006 ¶ 70 (emphasis added). And Petitioner itself argues only so far as to assert that "Chandnani *could be viewed* as teaching diversion of only script languages to its rule-based scanner." Pet. 34 (emphasis added). Such speculation as to how a person of skill in the art "could" have understood Chandnani is insufficient to support an anticipation challenge. *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987) ("A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.").

allowed to proceed to its intended destination or is diverted to the adaptive rule-based scanner for analysis. Ex. 1001, col. 19, ll. 30–42. Chandnani differs from this description, but the difference on which Patent Owner relies is not expressed in the claim. That is, Chandnani teaches diversion of incoming traffic, so that either a pattern-matching lexical analysis is performed or a CRC signature check is performed. Ex. 1013, col. 8, ll. 44–60. As such, diversion to the pattern-matching lexical analysis is "selective" according to the broadest reasonable interpretation of that term. Although the broadest reasonable interpretation is made in light of the specification, Patent Owner insufficiently articulates a reason to incorporate the particular kind of selectivity illustrated as an example in the Specification of the '305 patent. Patent Owner identifies no special definition of "selectively" provided by the Specification or other consideration that warrants limiting the claim language to be narrower than the plain and ordinary meaning of "selectively."

For these reasons, we determine that Petitioner also makes a sufficient showing with respect to this element.

We conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of independent claims 1, 13, and 25 as anticipated by Chandnani.

3. Dependent Claims 2, 3, 14, and 15

Claims 2 and 14, which depend respectively from claims 1 and 13, recite that "said database of parser and analyzer rules stores parser and analyzer rules in the form of pattern-matching engines." Ex. 1001, col. 30, ll. 47–49, col. 31, ll. 30–32. For this limitation, Petitioner observes that

"Chandnani expressly teaches that its 'lexical analysis may include one or more pattern matches based on the language definition rules.'" Pet. 36 (citing Ex. 1013, col. 3, ll. 52–53). Petitioner makes a sufficient showing with this identification, which is not disputed by Patent Owner outside its arguments directed at the base independent claims.

Claims 3 and 15, which depend respectively from claims 2 and 14, recite that "the pattern-matching engines are deterministic finite automata." Ex. 1001, col. 30, ll. 50–51, col. 31, ll. 33–34. For this limitation, Petitioner observes that "Chandnani describes that Dynamic Finite Automata may be used to conduct pattern matches, and corresponds to the 'deterministic finite automata' described for conducting pattern matches in the '305 patent." Pet. 37 (citing Ex. 1013, col. 3, ll. 55–60, col. 7, ll. 16–27; Ex. 1001, col. 11, ll. 15–19, col. 12, ll. 1–26; Ex. 1006 ¶ 76). Petitioner supports its contention, which is not disputed by Patent Owner outside its arguments directed at the base independent claims, with testimony by Dr. Spafford, which we credit for purposes of this Decision. Petitioner, thus, makes a sufficient showing for this limitation.

We conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of claims 2, 3, 14, and 15 as anticipated by Chandnani.

4. Dependent Claims 4 and 16

Claims 4 and 16 depend respectively from claims 2 and 14 recite that "the pattern-matching engines are non-deterministic finite automata." Ex. 1001, col. 30, ll. 52–53, col. 31, ll. 35–36. In addressing these limitations, which differ from claims 3 and 15 only in their recitation of

"non-deterministic finite automata," instead of "deterministic finite automata," Petitioner observes that "[t]he '305 patent describes that [deterministic finite automata] and [non-deterministic finite automata] 'are well known in the art of compilers as finite-state machines for pattern matching.'" Pet. 37 (citing Ex. 1001, col. 11, ll. 14–21). Petitioner makes a sufficient showing through its reasoning, supported by the testimony of Dr. Spafford, that a person of ordinary skill would thus have understood "that substitution of [nondeterministic finite automata] would have been obvious or obvious to try where exact evaluation of candidate rules is desired." *Id.* (citing Ex. 1006 ¶ 77).

We conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of claims 4 and 16 as rendered obvious over Chandnani.

5. Claims 5 and 17

Claim 5 depends from claim 1 and recites 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." Ex. 1001, col. 30, ll. 54–58. Claim 17 depends from claim 13 and similarly recites "preventing incoming content having a computer exploit that was recognized by said scanning from reaching its intended destination." *Id.* at col. 31, ll. 37–39. For these limitations, Petitioner identifies general teachings in Chandnani regarding an objective of virus-scanning programs to eliminate identified viruses, and provides testimony by Dr. Spafford that a person of ordinary skill would have understood from those teachings that

"the infected code would be prevented from executing at the destination computer." Pet. 38–39; Ex. 1006 ¶ 79. This reasoning is sufficient at this stage.

We conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of claims 5 and 17 as rendered obvious over Chandnani.

6. Claims 6–10 and 18–22

Claims 6–10 each depend from claim 1, and claims 18–22 each depend from claim 13, with each claim reciting that "the incoming content received from the Internet by said network interface" is "HTTP content," "HTTPS content," "FTP content," "SMTP content," or "POP3 content." Ex. 1001, col. 30, l. 59–col. 31, l. 6, col. 32, ll. 1–15. Chandnani discloses communication between a computer system and a network that includes "a LAN, a WAN, an intranet, an extranet, the Internet, and/or any combinations of such networks," which Dr. Spafford testifies "were notoriously well-known and in regular use by the effective filing date of the '305 patent." Ex. 1013, col. 4, ll. 49–51; Ex. 1006 ¶ 81. Petitioner makes a sufficient showing through its reliance on this evidence.

We conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of claims 6–10 and 18–22 as rendered obvious over Chandnani.

7. Claims 11, 12, 23, and 24

Claims 11 and 12 depend from claim 1, and claims 23 and 24 depend from claim 13, each reciting that the "destination Internet application" is "a

web browser" or "an e-mail client." Ex. 1001, col. 31, ll. 7–10, col. 32, ll. 16–19. Petitioner makes a sufficient showing for these limitations through its recognition, supported by testimony by Dr. Spafford, that a person of ordinary skill would have understood that the JavaScript files taught by Chandnani "generally were destined for a web browser or e-mail." Pet. 40–41 (citing Ex. 1006 ¶¶ 81, 84).

We conclude that Petitioner demonstrates a reasonable likelihood of prevailing on its challenge of claims 11, 12, 23, and 24 as rendered obvious over Chandnani.

C. Obviousness over Freund and Chandnani

We exercise our discretion and decline to institute review of claims 1–25 as unpatentable under 35 U.S.C. § 103(a) over Freund and Chandnani. 37 C.F.R. 42.108(a). As noted above, Freund was considered extensively by the Office during prosecution, including no fewer than five Office Actions in which the Examiner and Applicant negotiated the scope of the claims in light of the teachings of Freund. In light of that extensive prosecution history, we do not find it productive to reconsider patentability of the claims over Freund, even in combination with Chandnani, which Petitioner relies on for "types of tokens comprising a punctuation type, an identifier type and a function type" recited in independent claims 1, 13, and 25. *See* Pet. 41, 51–52. We agree with Patent Owner that Petitioner oversimplifies the prosecution history and that the Examiner considered other distinctions with Freund. *See* Prelim. Resp. 37–43.

Patent Owner requests that we sanction Petitioner for advancing this ground, and characterizes Petitioner's argument as "advanc[ing] a frivolous

argument, misrepresent[ing] facts, harass[ing] Patent Owner, and caus[ing] an 'unnecessary increase in the cost of the proceeding.'" Prelim. Resp. 13 (citing 37 C.F.R. §§ 42.12(a)(2), (3), and (7)). Although we agree that exercising our discretion to deny institution on this ground is warranted, we are not persuaded, based in part on our review of the prosecution history, that Petitioner's argument is so inappropriate as to rise to the level of sanctionable conduct. Accordingly, we decline to sanction Petitioner.

III. ORDER

It is

ORDERED that *inter partes* review is *instituted* with respect to whether claims 1–3, 13–15, and 25 are anticipated by Chandnani;

FURTHER ORDERED that *inter partes* review is *instituted* with respect to whether claims 4–12 and 16–24 would have been rendered obvious over Chandnani;

FURTHER ORDERED that *inter partes* review is *not instituted* with respect to any other ground of unpatentability; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(a), *inter partes* review of the '305 patent is hereby instituted, commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

PETITIONER:

Nicola A. Pisano
Christopher C. Bolten
FOLEY & LARDNER LLP
npisano@foley.com
cbolten@foley.com

PATENT OWNER:

Jeffrey H. Price
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jprice@kramerlevin.com