

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FINJAN HOLDINGS, INC.,
Petitioner,

v.

SOPHOS LIMITED,
Patent Owner.

Case IPR2015-01405
Patent 8,776,218 B2

Before HOWARD B. BLANKENSHIP, GREGG I. ANDERSON, and
WILLIAM M. FINK, *Administrative Patent Judges*.

ANDERSON, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Finjan Holdings, Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–20 of U.S. Patent No. 8,776,218 B2 (“the ’218 patent”), filed July 21, 2009. Sophos Limited (“Patent Owner”) elected not to file a Preliminary Response. On December 15, 2015, we granted the Petition and instituted trial on claims 1, 11, and 12 of the ’218 patent. Paper 9 (“Institution Decision” or “Dec. Inst.”).

After institution of trial, Patent Owner filed a Patent Owner Response (Paper 15, “PO Resp.”), and Petitioner filed a Reply (Paper 16, “Reply”). In addition, Petitioner proffered the Declaration and Reply Declaration of Dr. William Arbaugh (“Arbaugh Declaration,” Ex. 1020, “Arbaugh Reply Declaration,” Ex. 1025). The deposition of Dr. Arbaugh was taken by Patent Owner (“Arbaugh Deposition,” Ex. 2008). Patent Owner proffered the Declaration of Dr. Charles H. Sauer (“Sauer Declaration,” Ex. 2001). Dr. Sauer was not deposed.

An oral hearing was held on August 3, 2016. The transcript of the hearing has been entered into the record. Paper 36 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We conclude, for the reasons that follow, that Petitioner has shown by a preponderance of the evidence that claims 1, 11, and 12 of the ’218 patent are unpatentable.

A. *Related proceedings*

Petitioner advises that there are no judicial nor administrative matters pending involving the ’218 patent. Pet. 1.

B. The '218 patent (Exhibit 1001)

The '218 patent describes generally a method of “behavioral-based threat detection.” Ex. 1001, 1:7–8. The method includes “monitoring an executing computer process for [] indications of malicious behavior.” *Id.* at 1:43–47. The system compares monitored operations with predetermined behaviors, which the patent refers to as “gene[s],” to determine whether they indicate malicious behavior. *Id.* at 1:47–50.

The disclosed process collects multiple indications of malicious behavior together (i.e., collects particular genes) for comparison with predetermined collections of malicious behaviors that the patent refers to as “phenotype[s].” Ex. 1001, 1:52–54. Each “phenotype” is a collection of “genes” associated with a known type of malicious code. *Id.* at 1:54–56. The “phenotypes” are ranked to provide a level of confidence that the particular collection of behaviors indicates an actual attack. *Id.* at 18:26–30. If the confidence level is sufficiently high, the process triggers a content analysis and performs some other action such as pausing the process or displaying a message to the user. *Id.* at 18:49–64, 1:56–57.

C. Illustrative Claim

Of the challenged claims, claims 1 and 12 are independent. Claim 11 depends from claim 1. Claim 1 is reproduced below:

1. A computer program product embodied in a non-transitory computer readable medium that, when executing on one or more computers, performs the steps of:

monitoring an executing computer process for an indication of malicious behavior, wherein the indication of the malicious behavior is a result of comparing an operation with a predetermined behavior, referred to as a gene, where the gene is stored for reference in a database and wherein the gene relates to

at least one of API calls, registry access, process manipulation, and file system access;

performing the monitoring step a number of times to collect a plurality of malicious behavior indications;

comparing the plurality of malicious behavior indications to a predetermined collection of malicious behaviors, referred to as a phenotype, which comprises a grouping of specific genes that are typically present in a type of malicious code, and wherein the phenotype is one of a number of phenotypes that are ranked to create increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware;

triggering a content analysis of the executing computer process when the plurality of malicious behavior indications for the executing computer process corresponds to one of the number of phenotypes having a predetermined level of confidence that the executing computer process contains a known family of malware, thereby providing a prediction that the executing computer process is the type of malicious code; and

causing an action based on the prediction.

Ex. 1001, 23:60–24:24.

D. Instituted Grounds of Unpatentability

We instituted trial on the following grounds asserted by Petitioner under 35 U.S.C. § 103: (1) claims 1 and 12 as unpatentable over Lee¹ and Cooley;² (2) claim 11 as unpatentable over Lee, Cooley, and Tuvell;³ (3)

¹ US 7,809,670 B2, to Lee, issued October 5, 2010 (“Lee,” Ex. 1015).

² US 8,171,545 B1, to Cooley, filed February 14, 2007 (“Cooley,” Ex. 1017).

³ US 2007/0240217 A1, to Tuvell, published October 11, 2007 (“Tuvell,” Ex. 1003).

claims 1 and 12 as unpatentable over Farley⁴ and Cooley; and (4) claim 11 as obvious under 35 U.S.C. § 103(a) over Farley, Cooley, and Tuvell.

II. ANALYSIS

A. Claim Construction

In *inter partes* review, claim terms are given their broadest reasonable interpretation in light of the specification in which they appear.

Cuozzo Speed Techs., LLC v. Lee, 136 S. Ct. 2131, 2144–46 (2016); 37 C.F.R. § 42.100(b). Under the broadest reasonable construction standard, claim terms are generally given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth in the specification 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).

Petitioner identifies six terms for construction. Pet. 18–28. We construed all six terms in the Institution Decision. Inst. Dec. 6–9. Patent Owner proposes construction for one term, “are ranked.” PO Resp. 9–14. . We address the terms previously construed as well as “are ranked” below.

1. “gene” (Claims 1 and 11)

Petitioner asserts that a “gene” is a behavior. Pet. 18–19. Specifically, Petitioner points to claim 1, which recites in pertinent part,

⁴ US 7,089,428 B2, to Farley, issued August 8, 2006 (“Farley,” Ex. 1016).

“monitoring an executing computer process for an indication of malicious behavior, wherein the indication of the malicious behavior is a result of comparing an operation with a predetermined behavior, *referred to as a gene*.” *Id.* at 18 (citing Ex. 1001, 23:63–66). Petitioner also cites to portions of the Specification for support. *Id.* at 19 (citing Ex. 1001, 17:49–58; *see also id.* at 17:61–62, 17:67–18:3).

We rely on the claim language itself for our construction, as supported in the Specification. Based on that portion of the Specification cited by Petitioner, we construe “gene” to mean “an indication of malicious behavior of a computer process or operation.”

2. “*at least one of . . . and . . .*” (*Claims 1 and 12*)

Petitioner reproduces a portion of claim 1, which recites that “the gene relates to ***at least one*** of API calls, registry access, process manipulation, ***and*** file system access.” Pet. 19–20 (citing Ex. 1001, 24:1–3). Petitioner concludes this means that “at least one of” means either of the listed computer functions and not all listed functions. *Id.* at 20 (citing Ex. 1020 ¶ 113). According to Petitioner, any other result, i.e., one that relates to all of the recited functions, would be nonsensical. *Id.* (citing *AIA Eng’g Ltd. v. Magotteaux Int’l S/A*, 657 F.3d 1264, 1276 (Fed. Cir. 2001) (“We strive, where possible, to avoid nonsensical results in construing claim language.”)).

Petitioner also cites sections of the Specification as consistent with the proposed interpretation. *Id.* at 20–21 (citing Ex. 1001, 2:16–23, Ex. 1020 ¶ 114). Petitioner contends that dependent claim 10, for example, states that the “remedial action” of claim 9, from which claim 10 depends, “is at least one of” followed by types of remedial actions. *Id.* at 21 (citing Ex. 1001, 24:51–64). Petitioner concludes that “[o]ne of skill in the art would

understand the claim to require that the ‘remedial action’ be one or more of the actions in the list – not all of them.” *Id.* (citing Ex. 1020 ¶ 116).

Petitioner also cites to the file history for support. Pet. 21–22. In rejecting dependent claim 4, the Examiner states that “Tuvell teaches: the content analysis involves at least one of a genotype, a hashing, a partial matching, an emulation, and an interpretation and tokenisation.” *Id.* at 21 (citing U.S. App. Ser. No. 12/506,749, 175, (“’218 patent File History,” Ex. 1002) 70, 115, 148–49, 189).

We agree with Petitioner’s reasons and construe “at least one of . . . and” to mean in the alternative, any of the listed functions.

3. “phenotype” (*Claims 1 and 12*)

Petitioner asserts that a “phenotype” is a “collection of behaviors that is indicative of a type of malicious code.” Pet. 22 (citing Ex. 1020). Specifically, Petitioner points to claim 1, which recites in pertinent part, “comparing the plurality of malicious behavior indications to a predetermined collection of malicious behaviors, referred to as a phenotype, which comprises a grouping of specific genes that are typically present in a type of malicious code.” Ex. 1001, 24:6–10; *see also id.* at 25:10–17 (claim 12). Petitioner also cites to portions of the Specification for support. Pet. 23 (citing Ex. 1001, 18:16–26; *see id.* Abstract, 1:52–56, 18:4–7, 18:16–26, 18:30–36, 19:55–59).

We rely on the claim language itself for our construction, as supported in the Specification. Based on that portion of the Specification cited by Petitioner, we construe “phenotype” to mean “a predetermined collection of malicious behaviors of a computer process or operation.”

4. “*content analysis*” (claims 1 and 12)

Petitioner proposes that the term “content analysis” be construed as “analysis that is directed to the content of one or more files.” Pet. 23 (citing Ex. 1020 ¶ 122 (for the understanding of one of ordinary skill)). In support of its proposal, Petitioner cites to claim 1 as including the step of “triggering a content analysis of the executing computer process.” Ex. 1001, 24:16–17. Claim 12 is similar. Pet. 24 (citing Ex. 1001, 25:18–19). Petitioner also cites to dependent claims 4, 8, 15, and 19, which list different, alternative content analysis techniques. *Id.* (citing Ex. 1020 ¶ 123–25). Based on this record, we agree with Petitioner’s proposal and construe the term “content analysis” to mean “analysis that is directed to the content of one or more files.”

5. “*ranked*” (claims 1 and 12)

Petitioner proposes that the term “ranked” as used in claims 1 and 12 means ““ordered.”” Pet. 24. Petitioner repeats the pertinent portions of both claims which recite “wherein the phenotype is one of a number of phenotypes that are **ranked** to create increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware.” *Id.* (citing Ex. 1001, 24:11–15, 25:12–17).

On this record, we determine that Petitioner’s construction is consistent with the plain and ordinary meaning of “ranked” and requires no construction.

6. “*are ranked*” (claims 1 and 12)

Patent Owner contends that no construction beyond the ordinary meaning of “ranked” is necessary. PO Resp. 10. However, Patent Owner argues the “larger term ‘are ranked’” contained in the “comparing” step of

claims 1 and 12 should be “construed according to its plain and ordinary meaning as ‘are ranked *at the time the comparison is made.*’” *Id.* (citing Ex. 2001 ¶ 45) (emphasis added). Patent Owner then states that “[t]he plain and ordinary meaning of this limitation is that the phenotypes *are already ranked* at the time the comparing step is performed.” *Id.* at 11 (citing Ex. 2001 ¶ 47) (emphasis added).

Petitioner agrees that the plain and ordinary meaning of the words “are ranked” controls but, unlike Patent Owner, argues that no “further qualifying language” is required. Pet. Reply 3. Specifically, Petitioner argues that “are ranked” should be given its plain and ordinary meaning just like “ranked,” i.e., without a “temporal limitation.” *Id.* (citing Ex. 1025 ¶ 6).

Preliminarily, Patent Owner appears to propose two different timing qualifications to “are ranked,” at the time of the comparison step being performed and “already ranked” prior to the comparison step. *Compare* PO Resp. 21 (contending Lee does not teach “are ranked at the time the comparing step is performed”), *with* PO Resp. 23 (the construction of “are ranked” proposed by Petitioner is incorrect because it “does not require the number of phenotypes to already be ranked at the time the comparison is performed” (citing Ex. 2001 ¶ 62)).⁵ At the oral hearing, Patent Owner clarified and confirmed that “are ranked” required that the phenotypes are “already ranked.” *See* Tr. 31:4–32:21.⁶

⁵ Dr. Sauer’s testimony is likewise inconsistent as to when the ranking occurs. *Compare* Ex. 2001 ¶ 45 (“are ranked *at the time the comparison is made*”), *with* Ex. 2001 ¶ 47 (“the phenotypes are *already ranked at the time the comparing step is performed*”) (emphasis added).

⁶ A: “What we’re saying is that phenotype is *already ranked*. It has *got a ranking at the time you are making this comparison*. So what the patent

Patent Owner makes three arguments supporting inclusion of a temporal limitation into the term “are ranked.” Patent Owner first argues “are ranked” is a past participle form of the verb “to rank” and a part of the restrictive clause “that are ranked to create . . .” PO Resp. 11. Patent Owner concludes the use of “are ranked” refers to a complete action. *Id.* (citing A DICTIONARY OF MODERN LEGAL USAGE 765–67 (2d ed. 1987) (Ex. 2002, 7–9); MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY 907 (11th ed. 2003) (Ex. 2003, 4); Aim Publishing, *The Past Form and the Past Participle Form of Regular Verbs* (Ex. 2004)).

Petitioner argues Patent Owner’s position is not supported by the rules of grammar. Pet. Reply 4–7. Petitioner asserts the past participle form of a verb merely “signifies ‘perfectiveness’ or completion, but is not restricted to past time.” *Id.* at 4 (citing S. Chalker and E. Weiner, *THE OXFORD DICTIONARY OF ENGLISH GRAMMAR*, 286–87 (1994) (Ex. 1023); *see also id.* at 282 (past participle form of a verb “can be used for referring to past, present, or future time”); P. Peters, *The Cambridge Guide to English Usage*, 409 (2004) (“In traditional grammar terms, English has two participles, traditionally called present and past . . . The names present and past are misnomers, since either participle can occur in what is technically a present or past tense.”) (Ex. 1024)). Petitioner concludes “[t]he term ‘are ranked’ requires only that a number of phenotypes be ranked – it does not demand that the ranking occur at a particular point in time.” *Id.*

talks about in the comparison is doing a matching.” Tr. 32:5–8 (emphasis added).

We are not persuaded that the “rules of grammar” evidence of either party is definitive because the way the evidence is presented is contradictory. We begin our analysis with the words used in the claims. “The usage of the disputed claim terms in the context of the claims as a whole also informs the proper construction of the terms.” *Abbott Labs. v. Syntron Bioresearch, Inc.*, 334 F.3d 1343, 1351 (Fed. Cir. 2003) (citations omitted).

Claims 1 and 12 recite that “malicious behavior indications” are compared to “phenotypes,” as construed above. As a result of the comparison, the phenotypes “are ranked to create increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware.” It is only in the context of the comparison that the ranking occurs. There is no explanation in the specification or otherwise as to why the phenotypes would be ranked apart from and prior to the comparison being made. The reason for the comparison between the “malicious behavior indications” and the “phenotypes” is to identify the most problematic phenotype, which is “ranked” according to how similar it is to the “executing computer program.”

To the extent there is a grammar issue raised, we agree with Petitioner’s evidence that “the past participle form of a verb merely ‘signifies ‘perfectiveness’ or completion, but is not restricted to past time.’” Pet. Reply 4 (citing Ex. 1023, 282, 286–87; Ex. 1024, 409). This is consistent with our plain and ordinary meaning analysis immediately above.

Patent Owner’s second argument is based on the Federal Circuit’s decision in *Straight Path IP Group, Inc. v. Sipnet EU S.R.O.*, 806 F.3d 1356 (Fed. Cir. 2015). PO Resp. 12. *Straight Path* construed the phrase “is

connected to the computer network” to mean “is connected to the computer network at the time that the query is transmitted to the server.” *Straight Path*, 806 F.3d at 1363. Specifically, as to use of the past participle form, Patent Owner cites *Tuna Processors, Inc. v. Hawaii Int’l Seafood, Inc.*, 327 Fed. App’x. 204, 209–10 (Fed. Cir. 2009) as requiring a method steps be performed in sequential order. PO Resp. 12.

We agree with Petitioner that *Straight Path* supports a construction of “are ranked” as meaning that ranking is performed at the time of the comparing step. Pet. Reply 5–6. As Petitioner argues, applying *Straight Path*’s

logic here would require ‘are ranked’ to include ranking in the present (i.e., as part of the ‘comparing’ step). If Patent Owner’s argument that a past participle is limited to past activity were correct – if ‘are ranked’ actually meant ‘was ranked in the past’ – then the Federal Circuit would have construed the term ‘is connected’ to mean that the process was connected prior to the relevant step, which is precisely what the court rejected.

Id. at 6 (citing *Straight Path*, 806 F.3d at 1359–60). *Tuna Processing* is about the timing between separate steps, and is therefore inapposite here. Claims 1 and 12 do not recite a separate ranking step. Instead, ranking occurs as part of the comparing step.

Patent Owner’s third argument is that the specification of the ’218 patent supports its construction. PO Resp. 11, 14 (referencing PO Resp. 3–8). Dr. Sauer testifies that the ’218 patent’s description of a “threat research facility” that performs a “scaled analysis to create the predetermined ranked phenotypes is a process that is performed prior to the point in time in which the comparison of the unknown computer process is running and the comparison of those behaviors to the predetermined

phenotypes occurs.” Ex. 2001 ¶¶ 38–42, 48 (citing Ex. 1001, 11:34–41, 18:26–34); PO Resp. 11. We have reviewed the column 11 citation to the ’218 patent and find no support for concluding that the phenotypes are ranked prior to the comparison being made. *See, e.g.*, Ex. 1001, 11:34–37 (the threat management facility maintains threat protection capabilities). The column 18 reference to a “predetermined collection of behaviors” based on a “scaled analysis” suggests only that the collection of behaviors is predetermined, not that the ranking occurs prior to the comparison step itself.

Only one mention of “ranked” occurs in the specification, i.e., “[p]henotypes may capture a combination or a series of behaviors that may be ranked to create increasing levels of confidence that the runtime object being monitored is executing a behavior pattern comparable to a known family of malware.” Ex. 1001, 18:26–30. The cited description supports a construction of “are ranked” as occurring at the time of the comparison. Thus, the plain and ordinary meaning of “are ranked,” supported by the claims as a whole and the specification, is that the ranking of phenotypes may occur at the time the comparison is made. The argument of Patent Owner that phenotypes are “already ranked” prior to the comparison does not make sense when the claim as a whole is read because “[t]he purpose of ranking the phenotypes is to assess the risk that the runtime object is malware, not to assess the risk that the predetermined phenotype is malware.” Pet. Reply 10 (citing Ex. 1025 ¶ 11).

Dr. Sauer also relies on the file history as supporting an “already ranked” construction of “are ranked” because “the claimed products monitor the actual behavior of an executing process and compare it to a variety of

behaviors.” *Id.* ¶ 41 (citing Ex. 1002, 56); *see also* PO Resp. 8 (“phenotypes are created and ranked”). Patent Owner argues the comments show that the Applicant “expressly amended the ‘comparing’ and ‘triggering’ limitations . . . to more particularly require such ranking.” PO Resp. 8. Further, Patent Owner argues the cited comments from the ’218 patent File History are “almost verbatim” of the actual amendment made to claims 1 and 12. *Id.* The Arbaugh Reply Declaration includes testimony that “one of ordinary skill in the art would not understand the applicant’s comments to require that the creation of phenotypes and ranking of phenotypes necessarily happens at the same time or in advance.” Ex. 1025 ¶ 14 (citing Ex. 1002, 56); Pet. Reply 12.

As relevant to the ranking limitation, the actual amendment made to claim 1 added “and wherein the phenotype is one of a number of phenotypes that are ranked to create increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware” and deleted “wherein the phenotype is created based on a scaled analysis of families of malware.” Ex. 1002, 52. We agree that the “are ranked” language currently present in claim 1 was added over the prior “scaled analysis” language but do not agree that this amendment or the cited comment suggests that the ranking already occurred. We also agree with Petitioner that no argument was made in the ’218 patent File History that would support a construction of “are ranked” as requiring the ranking to occur prior to the comparing step. *See* Pet. Reply 12 n.2.

Petitioner’s evidence and argument do not preclude the ranking from occurring during the comparison step, i.e., at the same time. Thus, relying on the plain and ordinary meaning of “are ranked” as it appears in claims 1

and 12, we determine that “are ranked” may occur as part of the comparing step such that the phenotypes are not “already ranked.”

7. “*prediction*” (*claims 1 and 12*)

The term “prediction” is found in the “triggering” step as follows:

triggering a content analysis of the executing computer process when the plurality of malicious behavior indications for the executing computer process corresponds to one of the number of phenotypes having a predetermined level of confidence that the executing computer process contains a known family of malware, *thereby providing a prediction that the executing computer process is the type of malicious code...*

Ex. 1001, 24:16–23 (emphasis added); *see also id.* at 25:17–22 (claim 12 “triggering” step). Petitioner identifies two potential constructions based on the “thereby” clause. Pet. 26. According to Petitioner, the Specification supports its proposal that “prediction” means the “prediction is a result of the comparison to the phenotypes.” *Id.* (citing Ex. 1020 ¶ 130). The other alternative identified by Petitioner is the “prediction is a result of the triggering a content analysis.” *Id.*

On this record, we determine that Petitioner’s construction is consistent with the plain and ordinary meaning of “prediction” and requires no construction.

B. Obviousness Analysis

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying

factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

The parties’ positions on the level of ordinary skill in the art are substantially similar. Petitioner asserts a person of ordinary skill would have an undergraduate degree “in Computer Science or a comparable subject and at least five years of work experience in either the field of intrusion detection or in malware detection; or (ii) an advanced degree (or equivalent) in Computer Science or a comparable subject and at least one year of post-graduate research or work experience in either the field of intrusion detection or in malware detection.” Pet. 17–18 (citing Ex. 1020 ¶ 33). Patent Owner’s proposed level of ordinary skill is a “bachelor’s degree or the equivalent in computer science, computer engineering, or a related degree, and three to four years of experience in the field of Internet software, including anti-virus and other malware, or equivalent work experience.” PO Resp. 8–9 (citing Ex. 2001 ¶¶ 17–20).

Both proposals are similar in requiring at least an undergraduate degree and between three to five years of experience. Accordingly, we find that the person of ordinary skill has an undergraduate degree in computer science, computer engineering, or a related or comparable degree and at least four years of work experience in the field of Internet software, including anti-virus or intrusion or malware, detection, or equivalent work experience.

C. Obviousness over Lee, Cooley, and Tuvell

Petitioner alleges claims 1 and 12 would have been obvious to the person of ordinary skill in the art over Lee and Cooley. Pet. 32–47. Petitioner relies on the Arbaugh Declaration. *Id.* at 32 (citing Ex. 1020 ¶¶ 149–81 (claim 1), ¶¶ 182–97 (claim 12)). Petitioner also cites to claim charts in the Arbaugh Declaration. *Id.* (citing Ex. 1020 ¶ 198). The Arbaugh Declaration is also cited as evidence that one of ordinary skill in the art would have been motivated to combine Lee and Cooley. *Id.* (citing Ex. 1020 ¶¶ 199–205).

Petitioner alleges claim 11 would have been obvious to the person of ordinary skill in the art over Lee, Cooley, and Tuvell. Pet. 49–50. Petitioner alleges “[o]ne of skill in the art would have been motivated to, and could, combine Tuvell with Lee and Cooley for the same reasons discussed above.” *Id.* at 50 (citing Pet. 45–49; Ex. 1020 ¶¶ 257–260).

According to the Arbaugh Declaration, it is important to protect computer systems from malicious software or malware that makes unintended changes and even harms a computer system. Ex. 1020 ¶¶ 35–36. The ’218 patent, Lee, Cooley, and Tuvell are all directed to the identification, detection, and/or classification of computer programs as malicious code or malware. *See* Ex. 1001, 3:19–30; Ex. 1015, 4:3–13; Ex. 1017, 1:59–63; Ex. 1003 ¶ 2.

1. Lee (Exhibit 1015)

Lee classifies malware, disclosing a method and system for automatically classifying an application into an application group previously classified in a knowledge base. Ex. 1015, Abstract, 3:11–14. More specifically, a runtime behavior of an application is captured as a series of

events that are monitored and recorded during the execution of the application. *Id.* at Abstract, 3:14–17. The set of application groups “may be previously classified based on known malware applications and their runtime behaviors.” *Id.* at 4:1–3. Common “behavior patterns across malware variants or compilers and data/code variations within a malware family (group) can be detected.” *Id.* at 4:10–13.

Figure 2 of Lee is reproduced below.

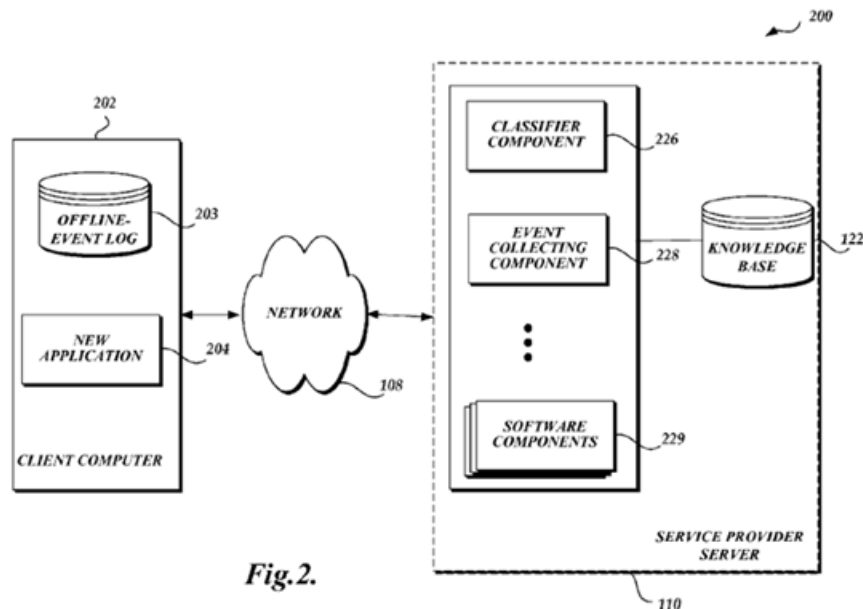


Fig.2.

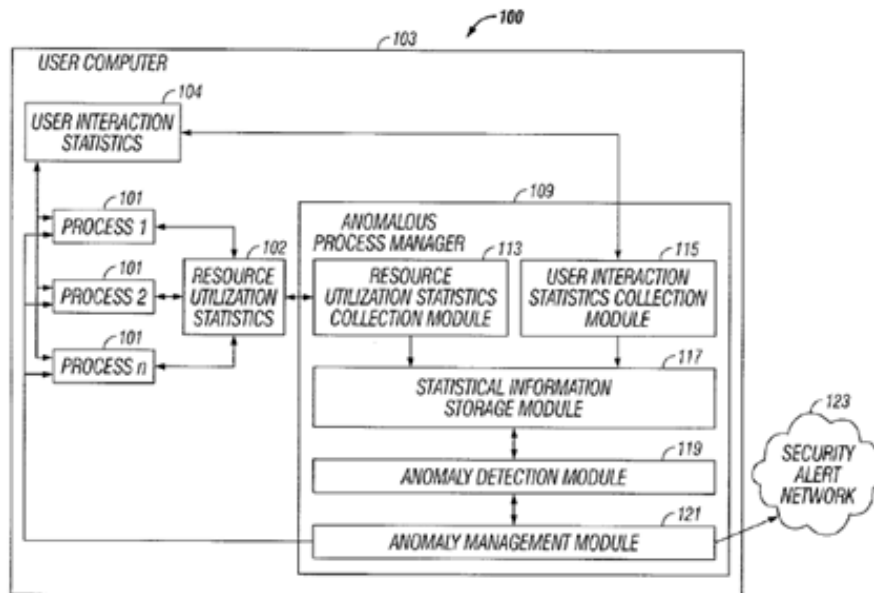
Figure 2 is a diagram of “an exemplary service provider server interacting with a client in accordance with embodiments of the present invention.” Ex. 1015, 2:59–61. As shown in Figure 2, new application 204 in the client computer may be evaluated by the knowledge base to determine whether the new application is one of the known malware family variants. *Id.* at 5:21–23. Each malware application may be represented in the form of sequenced events. *Id.* at 5:23–26. The knowledge base is constructed from the known event sequences of the known malware applications. *Id.* at 6:1–4.

In one embodiment, “the sample applications (e.g., known malware applications) are initially classified into several application groups, based on a defined distance measure which yields a similarity distance between two applications.” Ex. 1015, 6:15–19. The event sequence of the running application’s sequence of events is compared to the knowledge base to calculate the similarity distance. *Id.* at 6:23–25. “[C]lassifier component 226 may determine whether the new application can be classified into an application group with the closest (nearest) similarity distance.” *Id.* at 6:25–34. The server can “maintain a threshold value for the acceptable similarity distance among applications to form a group.” *Id.* at 6:38–40.

2. *Cooley (Exhibit 1017)*

Cooley describes “[a]n anomalous process behavior manager [that] uses statistical information concerning running processes to detect and manage process behavior anomalies.” Ex. 1017, Abstract. The anomalous process behavior manager “determine[s] whether processes are behaving in expected ways relative to past performance.” Ex. 1017, 1:52–57.

The sole unnumbered drawing figure of Cooley is reproduced below.



The above figure is a block diagram of the “anomalous process behavior manager 109” which “detects behavioral anomalies in applications 101 installed on a client computer 103 without requiring machine-external input.” Ex. 1017, 2:38–40. “The anomaly management module 121 takes appropriate action in response to a determination that a process 101 is behaving anomalously.” *Id.* at 5:49–51. Appropriate action “can consist of a simple notification user interface.” *Id.* at 5:60–63. Other actions include scanning the process for malicious code, closing the process’s network connections, suggesting to the user not to input financial information, uninstalling the process, or rolling back the process to an earlier version. *Id.* at 5:63–6:3.

3. Claims 1 and 12 (Lee and Cooley)-Petitioner’s Allegations

We first analyze claim 1, which Petitioner states is “very similar” to claim 12. See Pet. 15–17 (including side by side comparison chart). Patent Owner also argues claims 1 and 12 together. See PO Resp. 18, 20, 21, 23,

24, 27, 28, and 29 (each page containing a reference to “claims 1 and 12” or “claims 1 or 12”).

The preamble of claim 1 recites a “computer program product embodied in a non-transitory computer readable medium, that when executing on one or more computers, performs the steps of” Petitioner cites to both Lee and Cooley as disclosing computer implemented methods and programs. *Id.* at 33 (citing Ex. 1015, 1:66–2:2, Ex. 1017, 2:27–31).⁷

The first recited step of claim 1 is

monitoring an executing computer process for an indication of malicious behavior, wherein the indication of the malicious behavior is a result of comparing an operation with a predetermined behavior, referred to as a gene, where the gene is stored for reference in a database and wherein the gene relates to at least one of API calls, registry access, process manipulation, and file system access. . . .

This limitation is broken down and analyzed below.

Petitioner contends that “monitoring an executing computer process” is a dynamic analysis. Pet. 33–34 (citing Ex. 1020 ¶ 153). First, Petitioner alleges Lee is dynamic in that it captures the “runtime behavior of an application” which is “monitored and recorded during the execution of the application.” *Id.* at 34 (citing Ex. 1015, 3:14–17) (emphasis omitted). As to comparing operations with “a predetermined behavior,” Petitioner cites to Lee’s disclosure that “a set of specific events may be pre-defined to be captured for the clustering process of a particular knowledge base.” *Id.*

⁷ Here, and at several other places in the Petition, Petitioner cites to both Lee and Cooley as showing a specific limitation. Lee is advanced as the primary reference and, unless otherwise indicated, our limitation-by-limitation analysis is based on Lee alone. Cooley is analyzed where Petitioner relies solely on Cooley to meet the limitation.

(citing Ex. 1015, 5:50–54) (emphasis omitted). Lee also discloses constructing a “knowledge base of malware families.” *Id.* at 5:52–55. Petitioner concludes that Lee discloses monitoring “events” (i.e., “operations” of the executing process) and comparing them to “pre-defined events” (i.e., “genes”) as an indication of malicious behavior as per the monitoring limitation of claim 1. Pet. 34 (citing Ex. 1020 ¶ 154).

The monitoring limitation also recites that the “gene is stored for reference in a database” and that the “gene relates to at least one of API calls, registry access, process manipulation, and file system access.” Petitioner argues that Lee teaches a database of “predefined events” (i.e., genes), which includes “application groups and a set of application classifying rules where each application group has been classified based on the set of application classifying rules.” Pet. 35 (citing Ex. 1015, 2:25–30; Ex. 1020 ¶ 157). Relative to the functions listed, Lee is argued as disclosing “predefined events” or “genes” related to each of the four behaviors explicitly identified, including specifically registry open, registry write, registry query, file open, and file write. Pet. 36 (citing Ex. 1015, 5:55–59; Ex. 1020 ¶ 160).

Claim 1 next recites “performing the monitoring step a number of times to collect a plurality of malicious behavior indications.” Petitioner cites to Lee’s disclosure that “***a series of events and time information may be collected*** during the execution of the new application.” Pet. 37 (quoting Ex. 1015, 5:41–49). Petitioner also relies on Cooley, which discloses that “an anomalous process behavior manager ***collects per process statistical data over time . . .***” *Id.* (citing Ex. 1017, 1:52–59). Based on Lee alone or

in combination with Cooley, Petitioner concludes the “performing” step is disclosed. *Id.* (citing Ex. 1020 ¶ 166).

Claim 1 continues with a “comparing” step, i.e., “comparing the plurality of malicious behavior indications to a predetermined collection of malicious behaviors, referred to as a phenotype, which comprises a grouping of specific genes that are typically present in a type of malicious code.” Petitioner cites to Lee’s teaching that “the ***event sequence of the application may be compared with the event information of each application group***,” as disclosing this step. Pet. 37 (citing Ex. 1015, 6:23–25). Thus, Lee’s “event sequences” are compared to the “event information of each application group.” *Id.* (citing Ex. 1020 ¶¶ 168–69).

The comparing step also recites that “the phenotype is one of a number of phenotypes that are ranked to create increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware.” Petitioner argues this limitation is met by the comparison made in Lee between the application groups and the knowledge base in order to calculate “similarity distances.” Pet. 38 (citing Ex. 1015, 6:23–25; Ex. 1020 ¶ 171). The confidence level “ranking” that an application is malware is found, according to Petitioner, in the “similarity distance” and how close the distance is to a malicious code. *Id.* at 38–39 (citing Ex. 1015, 4:27–40, 6:10–22, 9:40–55; Ex. 1020 ¶ 172). Petitioner argues Lee allows for adjusting the “threshold” at which the similarity distance indicates malicious behavior, i.e., the recited “confidence level.” *Id.* at 39 (citing Ex. 1015, 9:45–53; Ex. 1020 ¶ 172).

The next step of claim 1 recites, in pertinent part, “triggering a content analysis of the executing computer process” when there is a “prediction that

the executing computer process is the type of malicious code.” Petitioner acknowledges Lee does not disclose this limitation but instead cites to Cooley’s disclosure that the “[t]he anomaly management module 121 takes appropriate action in response to a determination that a process 101 is behaving anomalously. . . . [T]he anomaly management console 121 can . . . scan the process and/or computer 103 for malicious code” Pet. 40 (citing Ex. 1017, 5:49–59). Petitioner argues the “behavioral analysis of Lee (and Cooley) and the content analysis of Cooley, alone and in combination with each other, provide a ‘prediction’ that the executing computer process is a type of malicious code.” *Id.* (citing Ex. 1020 ¶ 175).

Finally, claim 1 recites “causing an action based on the prediction.” Petitioner argues “Lee states that anti-malware analysts can evaluate the results and provide feedback or that an anti-malware application can be used to classify ‘unseen malwares.’” Pet. 41 (citing Ex. 1015, 10:18–22, 10:26–32). Citing the Arbaugh Declaration, Petitioner asserts the person of ordinary skill would have recognized there is no point in doing the analysis unless some action is taken. *Id.* (citing Ex. 1020 ¶ 180).

Aside from the comparing step, which we address below, Patent Owner does not dispute Petitioner’s mapping of Lee and Cooley to the limitations of claim 1. *See* II.C.5. *infra*. We determine that the foregoing evidence cited by Petitioner supports its contentions with respect to these limitations.

As previously noted, claim 12 is very similar to claim 1 and Petitioner cites to virtually the same disclosures relied on in connection with claim 1 to argue claim 12 is unpatentable. For example, Lee is cited as disclosing the “progressively monitoring” recitation of claim 12. Pet. 42–43. This

limitation is similar to claim 1's "monitoring" limitation. Petitioner cites to Lee's disclosure of collecting a plurality of malicious behavior indications, which was also cited in connection with the "monitoring" limitation. *See id.* (citing Ex. 1015, 5:41–52).

We have reviewed Petitioner's arguments and evidence applying Lee and Cooley to the balance of claim 12's limitations. Pet. 42–45. We have also reviewed the Arbaugh Declaration in connection with those same limitations. *See* Ex. 1020 ¶¶ 184, 188, 192. We specifically adopt Petitioner's reasoning and find by a preponderance of the evidence that Petitioner has shown the limitations of claim 12.

Petitioner also argues that the person of ordinary skill would have been motivated to combine Cooley with Lee. Pet. 45–47. In sum, Petitioner contends both Lee and Cooley relate to the same field of intrusion and malware detection. *Id.* at 45 (citing Ex. 1015, 1:24–56; 4:3–12; Ex. 1017, Abstract, 1:6–8, 1:52–57). Petitioner also asserts Lee and Cooley address the same problem of determining whether executing code is malicious. *Id.* (citing Ex. 1015, 4:3–12; Ex. 1017, 1:37–40). This is alleged to be the same problem addressed by the '218 patent. *Id.* at 45–46 (citing Ex. 1001, 1:32–36). Both Lee and Cooley detect malware via behavioral analysis and then a subsequent content analysis. *Id.* (citing Ex. 1020 ¶ 201). Petitioner concludes: the combination is a simple substitution; the benefit of the substitution would have been recognized by the person of ordinary skill; the substitution could be done without undue effort; and it would be obvious to try. *Id.* at 46–47 (citing Ex. 1020 ¶¶ 199–203, 205).

As discussed above, claim 12 has limitations similar to those of claim 1. For example, claim 1's "monitoring" step is performed "a number of

times” (Ex. 1001, 24:4–5) whereas claim 12 recites “progressively monitoring” (Ex. 1001, 25:4–5). We determine that the different language expresses the same step, monitoring more than one time. Similarly, both claims 1 and 12 include “comparing,” “triggering,” and “causing” steps. *Compare* Ex. 1001, 24:6–24 and Ex. 1001, 25:11–24. Thus, we agree with the parties’ arguments as noted above that there is no substantive difference between claims 1 and 12. Accordingly, we determine that Petitioner’s evidence supports its contentions with respect to the limitations of claim 12. The “comparing” step of claims 1 and 12 is addressed separately below in the context of the “are ranked” argument of Patent Owner. *See* II.C.5.b. *infra*.

4. Claim 11 (Lee, Cooley, and Tuvell)-Petitioner’s Allegations

Claim 11 depends from claim 1 and recites “wherein the gene is at least one of a system modification and a behavior of a process.” The Arbaugh Declaration asserts Tuvell discloses this limitation. Ex. 1020 ¶ 240 (citing Ex. 1003 ¶¶ 75–81, 92–99, Figs. 4, 7–9). We agree that at least paragraph 75 of Tuvell discloses a system for detecting malware in connection with the file system, monitors the directory of the operating system, and scans the associated directory for file changes.

Petitioner has also provided a rational basis for the combination of Lee, Cooley, and Tuvell. Pet. 49–50 (citing Ex. 1020 ¶¶ 257–260). Petitioner also references its prior argument for the combination of Lee and Cooley. *Id.* at 50 (citing Pet. 45–47).

5. Claims 1, 11, and 12 (Lee, Cooley, and Tuvell)-Patent Owner’s Response

Patent Owner advances two arguments directed to claims 1 and 12. First, Patent Owner argues Petitioner has failed to establish a motivation for

combining Lee and Cooley. PO Resp. 18–20. Second, Patent Owner argues that neither Lee nor Cooley show the “comparing” step of claims 1 and 12, specifically the “are ranked” recitation in the step. *Id.* at 20–24. Each argument is addressed below.

a. Motivation to Combine Lee and Cooley

Patent owner argues that Lee’s behavioral analysis would not have been combined with Cooley’s “binary determination” of malware detection and it would not have been obvious “to substitute Lee’s behavioral analysis for Cooley’s behavioral analysis because Lee’s behavioral analysis – as opposed to [‘]Cooley’s more binary determination of whether or not an application is malware – permits the combined system to determine whether an application is similar to a known family of malware.” PO Resp. 18 (citing Pet. 46; Ex. 2001 ¶ 55). Patent Owner argues that “Lee’s behavior analysis process is only performed when a new application is installed or begins to run for the first time.” *Id.* at 18–19 (citing Ex. 1015, 5:21–23, 5:32–39; Ex. 2001 ¶¶ 55–56).⁸ Patent Owner contends that Lee does not disclose performing the behavioral analysis at any other time than “when the application is new or first begins to run.” *Id.* at 19 (citing Ex. 2001 ¶ 56). Patent Owner argues Cooley, on the other hand, “discloses that its behavior analysis process monitors the applications ‘over time’ rather than at their start, to detect such changes.” *Id.* (citing Ex. 1017, 1:25–29, 1:52–54; Ex. 2001 ¶ 57).

⁸ The Sauer Declaration (Exhibit 2001) and the Patent Owner Response are virtually identical. The Sauer Declaration is not separately addressed here unless otherwise stated.

Based on the above distinctions and relying on the Sauer Declaration, Patent Owner concludes Cooley addresses a “worst of all” problem that occurs “long after startup.” PO Resp. 19–20 (citing Ex. 2001 ¶ 58). According to Patent Owner, because the Petition does not address this difference between the references in its argument that the two would have been combined, “the Petition fails to establish that substituting Lee’s behavior analysis for Cooley’s would have been obvious.” *Id.* at 20 (citing Ex. 2001 ¶ 58).

Patent Owner “recognizes that Lee does not precisely define for how long his monitoring occurs after an application begins to execute; i.e., how many behaviors are collected before the similarity distances are calculated.” PO Resp. 20 n.4 (citing Ex. 2001, 26 (¶ 58) n.2). Patent Owner also acknowledges “Cooley does not precisely define to what length of time ‘over time’ refers.” *Id.* Dr. Sauer summarizes this “how long” or “length of time” difference as “Lee monitors behaviors over a time period very much shorter than Cooley’s ‘over time.’” Ex. 2001 ¶ 58 n.2. We agree with Petitioner that “[t]he difference between Lee and Cooley cited by Patent Owner simply provides a further reason why one of ordinary skill in the art would be motivated to replace Cooley’s behavioral analysis with Lee’s behavioral analysis.” Pet. Reply 14 (citing Ex. 1025 ¶ 18).

We are not persuaded by Dr. Sauer’s testimony that substituting Lee’s behavior analysis for Cooley’s would not have been obvious to a person of ordinary skill in the art. Ex. 2001 ¶ 58. Dr. Sauer’s opinion is based on the length of time difference between Lee and Cooley and the related “worst of all” problem that occurs “long after startup.” Ex. 2001 ¶¶ 56–58; see PO Resp. 19–20. Neither Patent Owner nor Dr. Sauer persuades us that the

length of time differences between Lee and Cooley would have been of any significant consequence to the motivation of the person seeking to solve the problem of detecting malware. Thus, we determine that Dr. Sauer's conclusion is entitled to little weight.

We find the motivation for the combination is based on the undisputed fact that Lee and Cooley both use behavioral analysis to solve the same problem. This overlap between the problem and its solution is "a reason that would have prompted a person of ordinary skill in the art to combine the elements as the new invention does." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Both Lee and Cooley use behavioral analysis to address that problem and are interrelated.

Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate review, this analysis should be made explicit. As our precedents make clear, however, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.

Id. (internal citation omitted). Based on our findings concerning the interrelated teachings of Lee and Cooley, we determine that one of ordinary skill in the art would have had reason to combine Lee and Cooley or to substitute one technique for the technique used in the other.

b. The “are ranked” Limitation

Patent Owner alleges the Petition fails to establish that either Lee or Cooley⁹ discloses or suggests the “comparing” step. PO Resp. 20–21. Patent Owner alleges claims 1 and 12 both recite the comparing step, i.e., “wherein the phenotype is one of a number of phenotypes that **are ranked** to create increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware.” *Id.* at 21.

As noted above in II.A.6, Patent Owner argues both that the phenotype ranking is performed at the time of the comparison and that the phenotypes are already ranked at the time the comparison is performed. *Compare* PO Resp. 21, *with* PO Resp. 23. As previously addressed in the context of claim construction, these positions are inconsistent. *See also* Pet. Reply 18 n.3 (arguing two constructions are proposed by Patent Owner, one “an even narrower interpretation of its own proposed construction”). We proceed on the basis that Patent Owner argues the constructions in the alternative.

Patent Owner first argues, based on the ranking being performed at the time of the comparison, the Petition does not show the limitation because “the Petition asserts that the comparison occurs during calculation of similarity distances between observed behaviors and representative event sequences (predetermined phenotypes), and that the rank is the result of that

⁹ Patent Owner points out that Petitioner does not rely on Cooley for the comparing step. PO Resp. 21. We agree but fail to see the relevance. Petitioner relies on Lee for the comparing step. *See* Pet. 38–39; Pet. Reply 17–20.

calculation.” PO Resp. 22 (citing Pet. 38–39, 44; Ex. 2001 ¶ 61). We are not persuaded.

Petitioner’s argument and evidence support the assertion that the ranking in Lee is part of the comparison step and not “a result of the calculation.” See PO Resp. 22. For example, the Petition alleges “[i]n Lee, the ‘event sequence of the application [i.e., plurality of malicious behavior indicators]’ is ‘compared with the event information of each application group [i.e., a number of phenotypes] in the knowledge base in order to calculate similarity distances.’” Pet. 38 (citing Ex. 1015, 6:23–25; Ex. 1020 ¶ 171); see also Ex. 1020 ¶ 169; Ex. 1025 ¶ 24 (Lee ranks the “event sequences . . . at the time the comparing step is performed.”). Patent Owner cites this same language from the Petition, but fails to show how this language, or any other language quoted from the Petition or Dr. Arbaugh’s testimony, support its position. See PO Resp. 22–23 (citing Pet. 38–39; Ex. 1020 ¶ 172; Ex. 2001 ¶¶ 61–62).

Patent Owner supports its argument by emphasizing the following words from the Petition: “***in order to calculate similarity distances***”; “***the similarity distances***”; and “***provides a ranking***.” However, emphasis without explanation does not make Patent Owner’s argument persuasive. The citation to paragraph 61 of the Sauer Declaration is identical to the Patent Owner’s Response and adds nothing additional for our consideration.

Patent Owner’s alternative argument relies on its proposed construction of “are ranked” as requiring that “the number of phenotypes to already be ranked at the time the comparison is performed.” PO Resp. 23 (citing Ex. 2001 ¶ 62); see also *id.* at 23 n.5 (citing Ex. 2001, 29 (¶ 62) n.3). Patent Owner presents this argument based on the example in paragraph 172

of the Arbaugh Declaration, arguing in the example “similarity distances” in Lee are ranked and not the “representative event sequences,” i.e., the claimed phenotypes.” PO Resp. 24. Patent Owner misinterprets Dr. Arbaugh’s testimony. Dr. Arbaugh’s testimony does not rank “similarity distances” but rather uses the closeness of the “similarity distance” to “rank” which of “malicious application group” A or B is more or less similar to the application being analyzed. *See* Ex. 1020 ¶ 172. We fail to see how the fact that both A and B are “malware,” as Patent Owner asserts, differentiates Dr. Arbaugh’s example from claims 1 or 12. Indeed, A and B are both “phenotypes” which we have construed as “a predetermined collection of malicious behaviors of a computer process or operation.” *See* II.B.3 *supra*. Accordingly, we agree with Petitioner that “[t]he similarity distance between the observed behavior and each phenotype provides the ranking for that particular phenotype.” Pet. Reply 18 (citing Ex. 1015, 2:11–15; Pet. 38–39; Ex. 1020 ¶¶ 171–172; Ex. 1025 ¶ 25). Thus, Lee discloses ranking a number of “phenotypes.”

We have already rejected Patent Owner’s proposed construction of “are ranked” as meaning “already ranked.” *See* II.B.6 *supra*. We therefore find unpersuasive its argument based on “already ranked.” *See* PO Resp. 23.

Patent Owner questions that “the similarity distance could be the rank required by claims 1 and 12.” PO Resp. 23, *see also id.* at 23 n.5 (citing Ex. 2001, 29 (¶ 62) n.3). However, Patent Owner does not explain why and, in any event, assumes that Lee’s similarity distance is the ranking for purposes of making its “already ranked” argument. PO Resp. 23 n.5.

We specifically find that Lee’s “similarity difference” is a “ranking” that provides a confidence level that an application being analyzed is

malware depending on how close the “similarity distance” is to malicious code. *See* Pet. 38–39 (citing Ex. 1015, 4:27–40, 6:10–22, 9:40–55; Ex. 1020 ¶ 172).

c. Claim 11

Claim 11 depends from claim 1. Patent Owner does not make any separate argument that claim 11 is patentable over Lee, Cooley, and Tuvell. PO Resp. 29–30. Patent Owner relies on the arguments it advanced in connection with claim 1, which we found unpersuasive. *Id.* Petitioner has shown by a preponderance of the evidence that claim 11 is unpatentable over the combination of Lee, Cooley, and Tuvell. *See* Pet. 49 (citing Ex. 1003; 1002, 70–71, 114–15, 148–49 (where the Examiner rejected claim 11 based on Tuvell)).

6. Summary of Obviousness over Lee, Cooley, and Tuvell

As analyzed above, we adopt Petitioner’s rationale for combining Lee and Cooley and Lee, Cooley, and Tuvell. Pet. 45–47 (claims 1 and 11), 49–50 (claim 11). We also adopt Petitioner’s arguments that claims 1, 11, and 12 would have been obvious over Lee, Cooley, and Tuvell. *Id.* at 32–50.

On this record, and based on Petitioner’s evidence and arguments, Petitioner has shown by a preponderance of the evidence that claims 1 and 12 would have been obvious over Lee and Cooley. Petitioner has also shown by a preponderance of the evidence that claim 11 would have been obvious over Lee, Cooley, and Tuvell.

D. Obviousness over Farley, Cooley, and Tuvell

Petitioner alleges claims 1 and 12 would have been obvious to the person of ordinary skill in the art over Farley and Cooley. Pet. 50–59. Petitioner relies on the Arbaugh Declaration. *Id.* at 50 (citing Ex. 1020

¶¶ 261–294 (claim 1), ¶¶ 295–310 (claim 12). Petitioner also cites to claim charts in the Arbaugh Declaration. *Id.* (citing Ex. 1020 ¶ 311). The Arbaugh Declaration is also cited as evidence that one of ordinary skill in the art would have been motivated to combine Farley and Cooley. *Id.* (citing Ex. 1020 ¶¶ 312–317).

Petitioner alleges claim 11 would have been obvious to the person of ordinary skill in the art over Farley, Cooley, and Tuvell. Pet. 60. Petitioner alleges “[o]ne of ordinary skill in the art would have been motivated to, and could, combine Tuvell with Farley and Cooley for reasons similar to those discussed in connection with the combination of Lee and Cooley.” *Id.* (citing Pet. 49–50; Ex. 1020 ¶¶ 324–327).

As we discussed above, like the ’218 patent, Farley, Cooley, and Tuvell are all directed to the identification, detection, and/or classification of computer programs as malicious code or malware. *See* Ex. 1001, 3:19–30; Ex. 1016, 3:25–46; Ex. 1017, 1:59–63; Ex. 1003 ¶ 2.

1. Farley

Farley discloses a security management system that includes a “fusion engine” that detects relationships between raw events that may indicate malicious behavior. Ex. 1016, Abstract. Farley’s fusion engine can “rank the risk of real-time raw events as well as mature correlation events.” *Id.* at Abstract, 4:36–39. Individual security events are ranked according to risk and relationships between two or more security events are identified. *Id.* at 1:16–21.

Figure 2 of Farley is reproduced below.

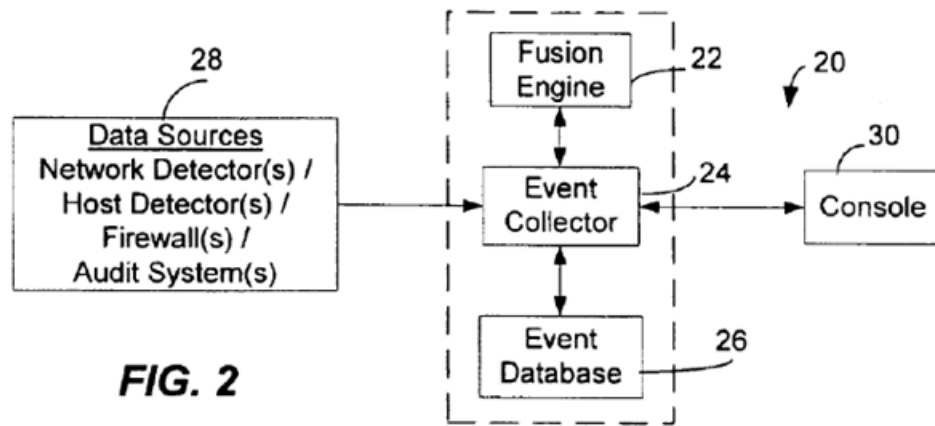


Figure 2 is a block diagram illustrating the network architecture of the Farley system. Ex. 1016, 5:23–24. Data source 28 is the host detector, a firewall or audit system. *Id.* at 9:61–65. One or more data sources forward their information to the event collector 24, which collects and stores the information. *Id.* at 10:9–13. Fusion engine 22 organizes and analyzes the information received from the data sources 28 to provide an organized presentation of information by correlating related computer events. *Id.* at 10:23–26. Once it is determined there is a correlation between two or more events, fusion engine 22 generates messages and forwards these messages to the event collector and then to console 30. *Id.* at 10:29–34.

In one embodiment the fusion engine uses correlation rules and the event categories defined in a Raw Event Classification Database to identify event patterns that indicate either malicious or nonmalicious activity. Ex. 1016, 20:33–38. The set of correlation events detected by the correlation rules includes, among other events listed: Attack from Attacked Host; Integrity Attack Followed By Remote Login; Sustained Availability Attack; Suspicious Activity Followed by Integrity Attack; and Sustained Confidentiality Attack. *Id.* at 20:40–22:24.

Parameters of each raw events logged by the fusion engine are compared with a context or knowledge base database. Ex. 1016, 23:48–55. Parameters are assigned to each raw event based upon a comparison with the knowledge database. *Id.* For example, “a sensor zone value 512 is assigned to each raw event based upon the sensor internet protocol address and a comparison with the context database 630.” *Id.* at 24:47–49. “The sensor zone value can comprise the internet protocol address of the sensor or detector of an intrusion detection system that detected the suspicious computer activity and generated the raw event.” *Id.* at 24:49–54.

2. *Claims 1 and 12 (Farley and Cooley)-Petitioner’s Allegations*

As above, we start with claim 1. The preamble of claim 1 recites a “computer program product embodied in a non-transitory computer readable medium, that when executing on one or more computers, performs the steps of” Petitioner cites to Farley as falling within the preamble because it is embodied in “program modules.” Pet. 50 (citing Ex. 1016, 6:16–17).¹⁰

The first recited step of claim 1 is

monitoring an executing computer process for an indication of malicious behavior, wherein the indication of the malicious behavior is a result of comparing an operation with a predetermined behavior, referred to as a gene, where the gene is stored for reference in a database and wherein the gene relates to at least one of API calls, registry access, process manipulation, and file system access. . . .

This limitation is broken down and analyzed below.

¹⁰ As discussed in footnote 5 above, Petitioner cites to both Farley and Cooley. Unless otherwise indicated, our limitation-by-limitation analysis is based on Farley alone. Cooley is analyzed only if Petitioner relies solely on Cooley to meet the limitation.

First, Petitioner alleges Farley discloses “executing [a] computer process” through its teaching that identifies relationships between computer events as they are received in real time. Pet. 50–51 (citing Ex. 1016, Abstract, 9:64–65; Ex. 1020 ¶ 263). Petitioner further notes that Farley describes suspicious computer activity as “real-time raw events.” *Id.* at 51 (citing Ex. 1016, 3:34–36) (emphasis omitted). Petitioner cites additional disclosures from Farley in support of its contention that Farley discloses the “monitoring step.” *Id.* (citing Ex. 1016, 4:18–20, 4:7–10). As to that portion of the monitoring step that recites comparing operations with “a predetermined behavior,” Petitioner cites to Farley’s disclosure of an “event database 26” that is linked to the “event collector 24.” Pet. 52 (Ex. 1016, 9:44–46); see Farley Fig. 2 above.¹¹

The monitoring limitation also recites that the “gene is stored for reference in a database” and that the “gene relates to at least one of API calls, registry access, process manipulation, and file system access.” Petitioner argues that Farley’s “audit system” tracks API calls and “would likely also include registry accesses, process manipulations and file system accesses.” Pet. 52–53 (citing Ex. 1016, 4:7–10, 9:64–65; Ex. 1020 ¶ 271).

¹¹ Petitioner also attempts to incorporate an additional reference, Houston (Ex. 1018), into its argument. Pet. 51–52 (citing Ex. 1016, 9:38–43, Ex. 1020 ¶ 265). Our rules prohibit arguments made in a supporting document from being incorporated by reference into a petition. See 37 C.F.R. § 42.6(a)(3). Furthermore, Houston is not relied on in a ground of unpatentability. Pet. 4. Separate references to Houston not contained in Farley will be given little weight beyond what it adds to the knowledge of a person of ordinary skill in the art. *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1365 (Fed. Cir. 2015).

Claim 1 next recites “performing the monitoring step a number of times to collect a plurality of malicious behavior indications.” Petitioner cites to Farley’s disclosure that “relationships between one or more real-time, raw computer events as they are received in real-time” as meeting the limitation. Pet. 53 (citing Ex. 1016, 10:21–23). Petitioner also cites to the “fusion engine” (see Figure 2 above) which “determines that **two or more events** are related to each other (to form a ‘correlation’ event).” *Id.* (citing Ex. 1016, 10:29–31). Petitioner concludes a “correlation event” is a plurality of malicious behavior indications. *Id.* (citing Ex. 1020 ¶ 275). Petitioner also relies on Cooley, which discloses collecting a plurality of malicious behavior indications. *Id.* (citing Ex. 1017, 1:52–59). Based on Farley alone or in combination with Cooley, Petitioner concludes the performing step is disclosed. *Id.* (citing Ex. 1020 ¶ 277).

Claim 1 continues with a “comparing” step, i.e., “comparing the plurality of malicious behavior indications to a predetermined collection of malicious behaviors, referred to as a phenotype, which comprises a grouping of specific genes that are typically present in a type of malicious code.” Petitioner cites to Farley’s teaching that whether a correlation event is a “mature correlation event,” indicating threats such as malware, is based on “correlation rules.” Pet. 54 (citing Ex. 1016, 4:18–31, 12:47–58, 20:8–18, Ex. 1020 ¶¶ 279–280).

The comparing step also recites that “the phenotype is one of a number of phenotypes that are ranked to create increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware.” As to the “ranking” limitation, Petitioner cites to Farley’s fusion engine which can “**rank** the risk of real-time raw

events as well as ***mature correlation events***.” Pet. 54 (citing Ex. 1016, 4:36–39, Ex. 1020 ¶¶ 282–283). Petitioner argues, and on this record we agree, that “mature correlation events” disclose the claimed “number of phenotypes.” *Id.*

The next step of claim 1 recites, in pertinent part, “triggering a content analysis of the executing computer process” when there is a “prediction that the executing computer process is the type of malicious code.” Based on the Arbaugh Declaration, Petitioner argues Farley discloses “a behavioral analysis that ranks phenotypes to provide an increased level of confidence that the runtime object is a type of malicious code.” Pet. 55 (citing Ex. 1020 ¶ 287). Petitioner also cites to Cooley (Ex. 1017, 5:49–59), as it did in the ground where Lee and Cooley were asserted, and to the Arbaugh Declaration to assert the “triggering” step is met. *Id.* (citing Ex. 1020 ¶ 289).

Finally, claim 1 recites “causing an action based on the prediction.” Petitioner argues Farley discloses “‘causing an action based on the prediction’ that an executing process is malicious.” Pet. 55 (citing Ex. 1016, 4:36–40). Citing the Arbaugh Declaration, Petitioner asserts the person of ordinary skill would recognize there is no point in doing the analysis unless some action is taken. *Id.* at 56 (citing Ex. 1020 ¶ 294).

As previously noted, claim 12 is very similar to claim 1 and Petitioner cites to virtually the same disclosures relied on in connection with claim 1 to argue claim 12 is unpatentable. We have reviewed Petitioner’s arguments and evidence applying Farley and Cooley to claim 12’s limitations. Pet. 56–58. We have also reviewed the Arbaugh Declaration in connection with those same limitations. See Ex. 1020 ¶¶ 295–310 and 311 (claim chart).

Aside from the comparing step, which we address below, Patent Owner does not dispute Petitioner’s mapping of Farley and Cooley to the limitations of claims 1 and 12. *See* II.D.4.a.–c. *infra*. We determine that the foregoing evidence cited by Petitioner supports its contentions with respect to these limitations.

Petitioner also argues that the person of ordinary skill would have been motivated to combine Cooley with Farley. Pet. 58–59 (citing Ex. 1020 ¶¶ 319–322). The arguments made, including field of endeavor, problem addressed, and ease of substitution, are similar to those we found persuasive in connection with the Lee and Cooley combination, and we also find those arguments persuasive for the combination of Cooley with Farley.

3. Claim 11 (Farley, Cooley, and Tuvell)-Petitioner’s Allegations

Patent Owner alleges claim 11 is unpatentable for reasons stated above in connection with claim 11 based on the combination of Lee, Cooley, and Tuvell. Pet. 60 (citing Pet. 49–50).

4. Claims 1, 11, and 12 (Farley, Cooley and Tuvell)-Patent Owner’s Response

Patent Owner makes three separate arguments, all of which are directed at the “comparing” step, specifically the “are ranked” limitation. PO Resp. 24–29. Each is addressed below.

a. Whether Farley Discloses Comparing the “plurality of malicious behavior indications” to “one of a number of phenotypes that are ranked” (Claims 1 and 12)

Petitioner cites to Farley’s teaching that “correlation events” are the claimed “plurality of malicious behavior indications” and correlation rules determine if the correlation event is indicative of a type of malicious code.

Pet. 54 (citing Ex. 1016, 4:18–31, 12:47–58, 20:8–18; Ex. 1020 ¶¶ 279–80). Further, Petitioner alleges that Farley’s “mature correlation event,” indicating threats such as malware, is a comparison of the “correlation event using correlation rules to determine if the correlation event is a collection of behaviors that are indicative of a type of malicious code.” *Id.* Patent Owner argues the preceding allegation of “correlation rules to the correlation event” as a comparison does not “identif[y] *anything* to which the correlation event is compared.” PO Resp. 26 (citing Ex. 2001 ¶ 68).

We disagree. As Petitioner alleges, the “correlation rules” compare correlation events with “event patterns that indicate either malicious or nonmalicious activity.” Pet. Reply 21 (citing Ex. 1016, 20:35–39); *see also* Pet. 54. We credit Dr. Arbaugh’s testimony that Farley employs “pattern matching (i.e., comparing) against information in a database to determine whether a correlation event is actually a ‘mature correlation event.’” Ex. 1025 ¶ 30 (citing Ex. 1016, 20:35–39). Thus, “Farley discloses – or, at a minimum, suggests to one of ordinary skill in the art – correlation rules that include comparing the observed correlation events with ‘event patterns that indicate either malicious or nonmalicious activity.’” *Id.* As Petitioner points out, there is a comparison as to whether or not an “immature correlation event” is a “mature correlation event,” based on “the level of confidence that the ‘runtime object is executing a behavior pattern comparable to a known family of malware.’” Pet. Reply 21 (citing Ex. 1025 ¶ 30).

b. *Whether Farley’s “mature correlation events” Discloses the Claimed “are ranked” to “create increasing levels of confidence” that the Events Indicate a “known family of malware” (Claims 1 and 12)*

The Petition alleges that Farley’s “mature correlation events” can be “ranked.” Pet. 54 (citing Ex. 1016, 13:13–15 (“In one exemplary embodiment, the fusion engine may track at least twenty different types of possible correlation events.”), 4:36–39 (“The fusion engine can also *assess and rank* the risk of real-time raw events as well as mature correlation events.”) (emphasis added); Ex. 1020 ¶¶ 282–283). Patent Owner argues the “risk” is based on the context, e.g., vulnerability information, historical event frequency information, and predefined network zones, in which the event is occurring. PO Resp. 28 (citing Ex. 1016, 18:31–43, 23:48–24:54, 23:61–24:16, Figs. 7, 10; Ex. 2001 ¶ 69). Patent Owner concludes that Farley does not “disclose that the relevant context includes any level of confidence that an event belongs to any malware family” and does not establish that the “‘mature correlation events’ are ranked according to increasing levels of confidence that they belong to a malware family.” *Id.* (citing Ex. 2001 ¶¶ 69–70).

We agree with Petitioner that Patent Owner’s argument assumes incorrectly “that phenotypes must be ranked in advance and not ‘in the environment or context in which the event occurred’ (as they are in Farley).” Pet. Reply 22 (citing Ex. 1025 ¶ 32). Patent Owner’s argument is consistent with its proposed construction of “are ranked,” which we rejected. We are also persuaded that there is no difference between assessing a level of confidence that there is a risk to a computer system and developing a level of confidence that the risk is a result of malware. *See id.* Similarly, we

agree with Petitioner that “[o]ne of ordinary skill in the art would understand, and find obvious, the fact that malware is only malware if it poses a risk of harm to the computer system.” *Id.*

c. Whether Farley’s “mature correlation events” Discloses the Claimed “are ranked” at the time the Comparing step is Performed (Claims 1 and 12)

Patent Owner argues the Petition “does not cite anything in Farley that indicates when that ranking occurs.” PO Resp. 28–29 (citing Ex. 1016, 4:36–39; Ex. 2001 ¶ 71). Patent Owner also argues the Petition asserts that “it is *mature* correlation events that Farley’s system ranks, it is clear that the ranking must occur after the comparison step occurs.” *Id.* at 29 (citing Ex. 2001 ¶ 71). Dr. Sauer testifies that “because the Petition asserts that it is *mature* correlation events that Farley’s system ranks, it is clear that the ranking must occur after the comparison step occurs.” Ex. 2001 ¶ 71.

We are not persuaded by Patent Owner’s arguments. First, we are not persuaded to the extent the argument is based on Patent Owner’s argument about the construction of “are ranked,” which we rejected. *See* II.B.6 *supra*; Pet. Reply 22.

Second, we disagree that Farley’s ranking occurs after the comparison step. The only evidence Patent Owner offers is Dr. Sauer’s testimony, which relies on the word “mature” as indicating some time has passed before a “mature correlation event” exists and can be ranked. *See* Ex. 2001 ¶ 71. Patent Owner does not cite to anything else in Farley for support. Indeed, Farley discloses that “mature correlation events” are “suspicious computer activity descriptions obtained from data sources as real-time raw events and actual computer security threats.” Ex. 1016, 3:34–37. Nothing in this

description suggests the temporal component Patent Owner argues is required.

Additionally, Patent Owner “effectively concedes that Farley does not specify when the ranking occurs.” Pet. Reply 22 (citing PO Resp. 29); see Ex. 2001 ¶ 71. We agree that Farley suggests to the person of ordinary skill in the art that mature correlation events can be ranked after the “comparing” step or as part of the “comparing” step. See Pet. Reply 22 (citing Ex. 1025 ¶ 33). We agree “Farley is not limited to either approach.” *Id.* As Petitioner argues, “the fact that the individual raw events are themselves ranked as they are collected suggests that their rankings would be used in the process of identifying mature correlation events as part of the ‘comparing’ step, not after the ‘comparing’ step.” *Id.* Accordingly, we find that Farley does suggest ranking during the comparing step.

d. Claim 11-Patent Owner’s Position

Claim 11 depends from claim 1. Patent Owner does not make any separate argument that claim 11 is patentable over Farley, Cooley, and Tuvell. PO Resp. 29–30. Patent Owner relies on the arguments it advanced in connection with claim 1, which arguments we found unpersuasive. Petitioner has shown by a preponderance of the evidence that claim 11 is unpatentable over the combination of Farley, Cooley, and Tuvell. See Pet. 60 (citing Ex. 1020 ¶¶ 323–327; Pet. 49–50).

5. Summary of Obviousness over Farley, Cooley, and Tuvell

As analyzed above, we adopt Petitioner’s rationale for combining Farley and Cooley and Farley, Lee, and Tuvell. See Pet. 58–59 (Farley and Cooley), 60 (Farley, Cooley, and Tuvell). We also adopt Petitioner’s

arguments that claims 1, 11, and 12 would have been obvious over Farley, Cooley, and Tuvell. *Id.* at 50–58, 60.

On this record, and based on Petitioner’s evidence and arguments, we determine that Petitioner has shown by a preponderance of the evidence that claims 1 and 12 would have been unpatentable over Farley and Cooley and that claim 11 would have been unpatentable over Farley, Cooley, and Tuvell.

III. ORDER

For the reasons given, it is:

ORDERED that claims 1, 11, and 12 of U.S. Patent No. 8,776,218 B2 have been shown by a preponderance of the evidence to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

James L. Day
FARELLA BRAUN & MARTEL LLP
jday@fbm.com

PATENT OWNER:

James Heintz
Jeff Cole
sophos-finjan-218IPR@dlapiper.com