

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.,
Petitioner,

v.

TAASERA LICENSING LLC,
Patent Owner.

IPR2023-00798
Patent 8,850,517 B2

Before JAMES P. CALVE, JUSTIN T. ARBES, and
ARTHUR M. PESLAK, *Administrative Patent Judges*.

ARBES, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

Petitioner Trend Micro, Inc. filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–24 of U.S. Patent No. 8,850,517 B2 (Ex. 1001, “the ’517 patent”) pursuant to 35 U.S.C. § 311(a). Patent Owner Taasera Licensing LLC filed a Preliminary Response (Paper 6, “Prelim. Resp.”) pursuant to 35 U.S.C. § 313.

Pursuant to 35 U.S.C. § 314(a), the Director may not authorize an *inter partes* review unless the information in the petition and preliminary response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” *See* 37 C.F.R. § 42.4(a) (“The Board institutes the trial on behalf of the Director.”). For the reasons that follow, we institute an *inter partes* review as to claims 1–24 of the ’517 patent on all grounds of unpatentability asserted in the Petition.

B. Related Matters

The ’517 patent also is the subject of Case IPR2023-00704 (“the -704 case”), filed by a different petitioner. *See* Pet. 69; Paper 3, 2. A decision granting institution of *inter partes* review in the -704 case was entered on October 13, 2023. IPR2023-00704, Paper 11 (“-704 Dec. on Inst.”). The parties also identify *In re Taasera Licensing, LLC, Patent Litigation*, No. 2:22-md-03042 (E.D. Tex.) (“the district court case”), in which the ’517 patent is asserted against a number of defendants, including Petitioner. *See* Pet. 69; Paper 3, 2. Another petitioner also filed a petition challenging claims of the ’517 patent in Case IPR2023-01465.

C. The ’517 Patent

The ’517 patent, titled “Runtime Risk Detection Based on User, Application, and System Action Sequence Correlation,” relates to “assessing the runtime risk of an application or device in a computer system using cognitive behavior recognition.” Ex. 1001, code (54), col. 1, ll. 7–10. The ’517 patent states that “computer and cyber security has become increasingly important,” but that “[e]merging cyber threats, commonly

referred to as advanced persistent threats (APT), often remain undetected using traditional security programs and approaches.” *Id.* at col. 1, ll. 14–29. According to the ’517 patent, the disclosed system and method addresses “a need for a technical solution to properly detect and prevent attacks by advanced persistent threats” in computer devices “undetected using traditional security programs and approaches.” *Id.* at col. 1, ll. 36–39.

Figure 1 of the ’517 patent is reproduced below.

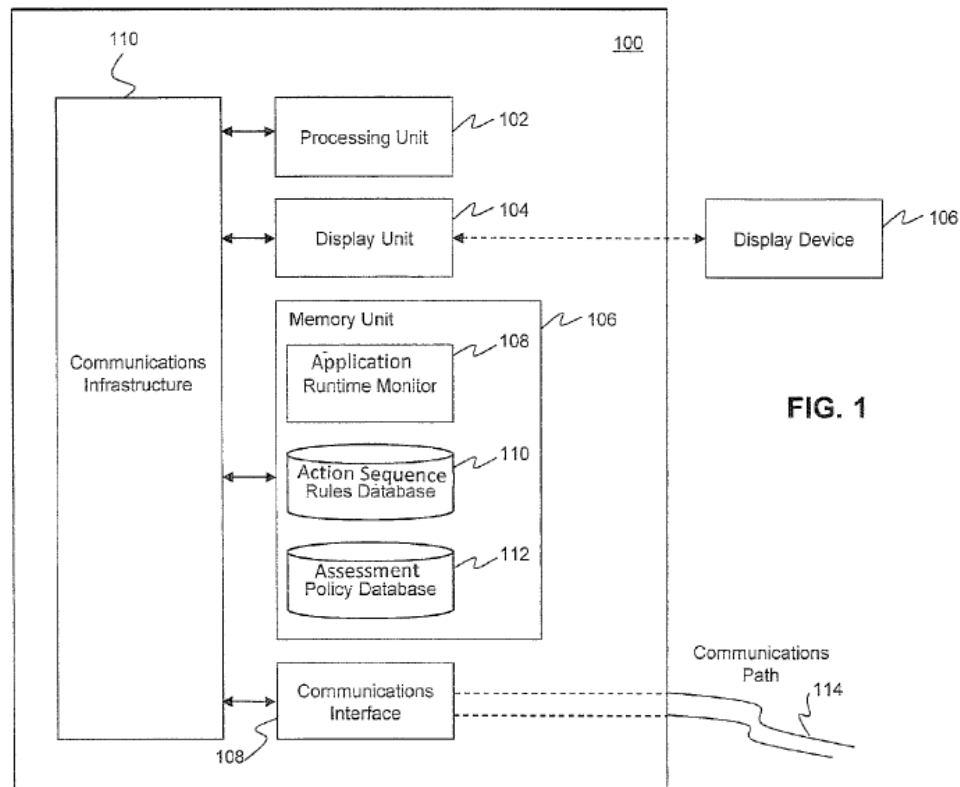


Figure 1 is a block diagram of a system for assessing the runtime risk for an application or device. *Id.* at col. 2, ll. 16–18. As shown in Figure 1, computing system 100 includes processing unit 102, display unit 104, memory unit 106, and communications interface 108 connected to communications infrastructure 110. *Id.* at col. 2, ll. 55–65, col. 3, ll. 3–4, col. 3, ll. 21–22, col. 4, ll. 43–45. Memory unit 106 includes runtime

monitor 108, rules database 110, and policy database 112. *Id.* at col. 3, ll. 38–39.

Runtime monitor 108 “may be an application program” that is “configured to assess the runtime risk of an application (e.g., stored in the memory unit 106 and executed by the processing unit 102) or device (e.g., connected to the computing system 100 externally (e.g., via the communications interface 108) or internally (e.g., via the communications infrastructure 110)[)].” *Id.* at col. 3, ll. 43–51. The runtime monitor may also be “configured to identify a behavior score for an action sequence of at least two performed actions executed by (e.g., by components or programs included in) the computing system 100.” *Id.* at col. 3, ll. 51–55.

Rules database 110 stores a plurality of rules, where each rule identifies an “action sequence.” *Id.* at col. 4, ll. 12–14. The ’517 patent states that an action sequence “include[s] a sequence of at least two performed actions, wherein the performed actions may be one of a user action, an application action, and a system action.” *Id.* at col. 4, ll. 14–17. Policy database 112 stores a plurality of assessment policies, where each assessment policy includes “at least one rule of the plurality of rules stored in the rules database.” *Id.* at col. 4, ll. 17–21.

The ’517 patent describes a “user action” as any form of explicit input from a user (e.g., program launch, keyboard input, mouse click, touch on a touchscreen), an “application action” as any activity performed by the application (e.g., a start type, first time execution, fork process), and a “system action” as any operation performed by the computing system “on behalf[of], or as a consequence of, an application or user action that changes the state of the computing system” (e.g., system file creation, system folder

modification, registry modifications or additions). *Id.* at col. 6, l. 56–col. 7, l. 26.

Figure 4 of the '517 patent is reproduced below.

400

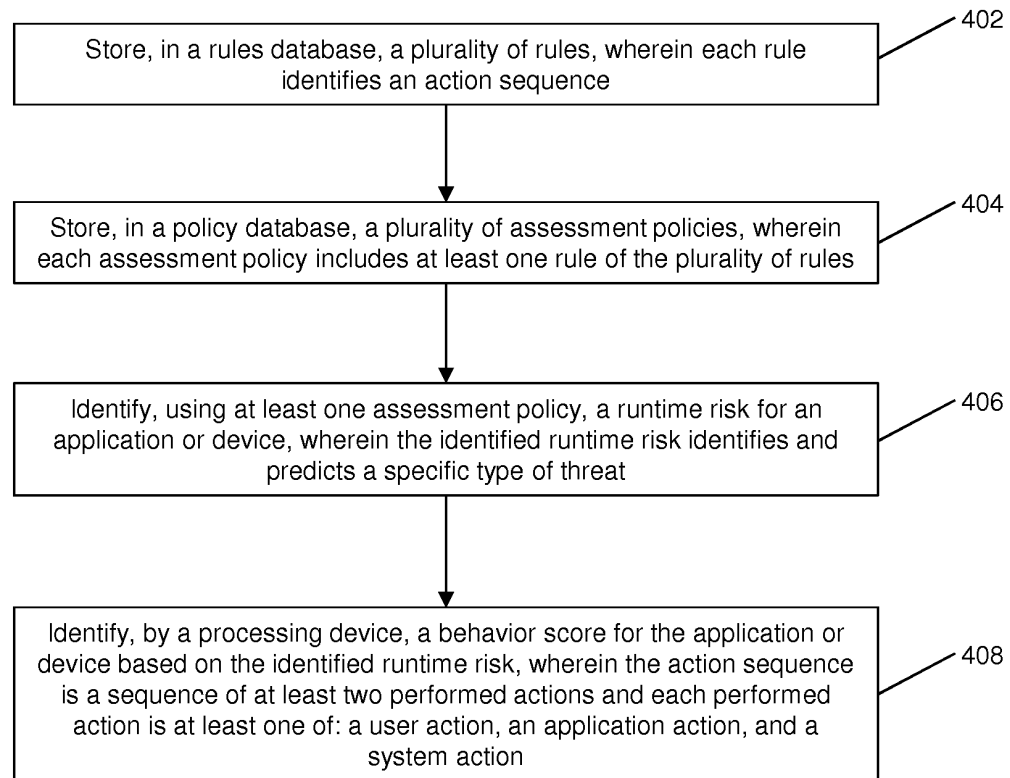


Figure 4 is a flow diagram of a method for assessing the runtime risk for an application or device. *Id.* at col. 8, ll. 56–60. In steps 402 and 404, a plurality of rules is stored in the rules database and a plurality of assessment policies is stored in the policy database, respectively. *Id.* at col. 8, ll. 61–col. 9, l. 4. In step 406, the runtime monitor identifies a runtime risk (i.e., a specific type of threat) for an application or device “using at least one assessment policy.” *Id.* at col. 9, ll. 5–8. The '517 patent states that in one embodiment, a runtime risk is identified “based on matching rules and probabilistic weights,” and, in another embodiment, a runtime risk is identified “based on time proximity of the at least two

performed actions of the action sequence and natural affinity inferred between the at least two performed actions.” *Id.* at col. 9, ll. 8–13. Finally, in step 408, the processing device identifies a behavior score for the application or device “based on the identified runtime risk.” *Id.* at col. 9, ll. 13–16.

D. Illustrative Claim

Challenged claims 1 and 13 of the ’517 patent are independent. Claims 2–12 depend, directly or indirectly, from claim 1, and claims 14–24 depend, directly or indirectly, from claim 13. Claim 1 recites (with letter designations used in the Petition to refer to the various limitations):

1. [a] A method for assessing runtime risk for an application program that executes on a device, comprising:

[b] storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence;

[c] storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules;

[d] identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application; and

[e] identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk, wherein

[f] the action sequence is a sequence of at least two performed actions, and

each performed action is at least one of: a user action, an application action, and a system action.

E. Evidence

Petitioner relies on the following prior art:

U.S. Patent No. 8,806,647 B1, filed Apr. 27, 2012, issued Aug. 12, 2014 (Ex. 1006, “Daswani”); and

U.S. Patent Application Publication No. 2011/0023115 A1, published Jan. 27, 2011 (Ex. 1005, “Wright”).

F. Prior Art and Asserted Ground

Petitioner asserts that claims 1–24 of the ’517 patent are unpatentable over Wright and Daswani under 35 U.S.C. § 103(a).¹

II. ANALYSIS

A. Discretionary Denial Under 35 U.S.C. § 314(a)

Institution of *inter partes* review is discretionary. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) (“[T]he PTO is permitted, but never compelled, to institute an [*inter partes* review (IPR)] proceeding.”); 35 U.S.C. § 314(a) (“The Director *may not* authorize an *inter partes* review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” (emphasis added)).

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the challenged claims of the ’517 patent have an effective filing date before the effective date of the applicable AIA amendment, we refer to the pre-AIA version of 35 U.S.C. § 103. *See* Pet. 3.

The Board has held that the advanced state of a parallel district court action is a factor that may weigh in favor of denying a petition under § 314(a). *See NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (precedential) (“*NHK*”); Patent Trial and Appeal Board Consolidated Trial Practice Guide (Nov. 2019), 58 & n.2, *available at* <https://www.uspto.gov/TrialPracticeGuideConsolidated>. We consider the following factors to assess “whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding”:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board’s exercise of discretion, including the merits.

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11 at 5–6 (PTAB Mar. 20, 2020) (precedential). In evaluating these factors, we “take[] a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *Id.* at 6.

In its Preliminary Response, Patent Owner argues that we should exercise our discretion to deny the Petition in view of the district court case. Prelim. Resp. 25–33. Patent Owner contends that trial in the district court case is scheduled for before our deadline for a final written decision in this

proceeding, “the parties (and Patent Owner in particular) have invested significant resources on developing legal and factual issues of validity and infringement in the [district court case] and will have invested substantially more resources before any decision on this Petition,” and “Petitioner has raised substantially similar, if not identical, arguments” in the district court case as it does in this proceeding. *Id.* at 25–26.

Petitioner argues that the district court case is still at an “early” stage and its preliminary invalidity contentions do not include the two references asserted in this proceeding, Wright and Daswani. Pet. 67. Petitioner also “stipulates that, if the Board institutes trial in this IPR, Petitioner will not pursue, in the [district court case], the specific grounds asserted in the IPR petition, nor any ground based on any prior art reference asserted in the IPR petition.” Paper 7.

On November 27, 2023, the district court issued an Order granting a Joint Motion to Stay All Deadlines and Notice of Settlement filed by the parties in the district court case. Ex. 3001. The Order states that “the parties represent that they have reached a settlement in principle and request a stay of all case deadlines for thirty-five days for the parties to finalize such settlement and file dismissal papers with the Court.” *Id.* The parties also notified the Board of the settlement and timing with respect to the Joint Motion by email on November 27, 2023. Given the parties’ settlement in the district court case, there will be no trial of Patent Owner’s asserted claims against Petitioner in the district court case, and thus there is no basis to deny institution under § 314(a). We decline to exercise our discretion to deny the Petition.

B. Legal Standards

A claim is unpatentable for obviousness if, to one of ordinary skill in the pertinent art, “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.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a) (2006)). The question of obviousness is resolved on the basis of underlying factual determinations, including “the scope and content of the prior art”; “differences between the prior art and the claims at issue”; and “the level of ordinary skill in the pertinent art.” *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Additionally, secondary considerations, such as “commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.” *Id.* When conducting an obviousness analysis, we consider a prior art reference “not only for what it expressly teaches, but also for what it fairly suggests.” *Bradium Techs. LLC v. Iancu*, 923 F.3d 1032, 1049 (Fed. Cir. 2019).

A patent claim “is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.” *KSR*, 550 U.S. at 418. An obviousness determination requires finding “both ‘that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.’” *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016); *see KSR*, 550 U.S. at 418 (for an obviousness analysis, “it can be important to identify a reason that would have prompted

a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does”).

“Although the *KSR* test is flexible, the Board ‘must still be careful not to allow hindsight reconstruction of references . . . without any explanation as to *how* or *why* the references would be combined to produce the claimed invention.’” *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1066 (Fed. Cir. 2016). Further, an assertion of obviousness “cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); accord *In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (stating that “conclusory statements” amount to an “insufficient articulation[] of motivation to combine”; “instead, the finding must be supported by a ‘reasoned explanation’”); *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.”).

C. Level of Ordinary Skill in the Art

Petitioner argues that at the time of the ’517 patent (January 2013), a person of ordinary skill in the art would have had “a bachelor’s degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one to two years of education or experience in the field of computer security,” where “[m]ore education can supplement practical experience and vice versa.” Pet. 7–8 (citing Ex. 1003 ¶ 87). Patent Owner adopts Petitioner’s definition for purposes of

its Preliminary Response. Prelim. Resp. 12. Based on the record presented, including our review of the '517 patent and the types of problems and solutions described in the '517 patent and cited prior art, we agree with Petitioner's proposed definition of the level of ordinary skill in the art and apply it for purposes of this Decision. *See, e.g.*, Ex. 1001, col. 1, ll. 5–39. We note that a slightly different definition was adopted in the -704 case (“a bachelor's degree in computer science or computer engineering, or an equivalent field and at least two to three years of experience in computer and network security”). *See* -704 Dec. on Inst. 16–17. Our conclusions herein, however, would be the same if that definition is used.

D. Claim Interpretation

We interpret each challenged claim

using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b). Petitioner does not propose interpretations of any claim terms. Pet. 8. Patent Owner only notes that the parties agreed in the district court case that the term “runtime” in claims 1, 10, 13, and 22 means “the time the application is running.” Prelim. Resp. 11 (citing Ex. 2003, 45–54). No claim terms were interpreted in the -704 case. *See* -704 Dec. on Inst. 17–18. We conclude that no express claim interpretation is necessary to determine whether to institute an *inter partes* review in this proceeding. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“Because we need only construe terms ‘that are

in controversy, and *only to the extent necessary* to resolve the controversy,’ we need not construe [a particular claim limitation] where the construction is not ‘material to the . . . dispute.’” (citation omitted) (emphasis added)).

E. Obviousness Ground Based on Wright and Daswani (Claims 1–24)

Petitioner contends that claims 1–24 are unpatentable over Wright and Daswani under 35 U.S.C. § 103(a), citing the testimony of Seth James Nielson, Ph.D., as support. Pet. 8–66 (citing Ex. 1003). Patent Owner disputes whether the asserted references teach certain limitations of the independent claims. Prelim. Resp. 13–24. We are persuaded that Petitioner has established a reasonable likelihood of prevailing on its asserted ground as to independent claims 1 and 13.

1. Wright

Wright discloses a “behavioral-based host-intrusion prevention method and system” for “monitoring a user interaction with a computer, software application, operating system, graphic user interface, or some other component of a computer (e.g. a client) within a computer network” and “performing an action to protect the computer and/or computer network based at least in part on the user interaction.” Ex. 1005 ¶ 7. Wright’s system (1) monitors user interaction (e.g., “executing a link,” “downloading a content item from a server,” “updating an application”) for an “indication of a user behavior” and (2) monitors actions that occur during an executing computer code process (e.g., “system startup, login, scheduled job process”) for an “indication of a code operation.” *Id.* ¶¶ 7, 10, 13. “The indication of the user behavior may be a result of comparing the user interaction, or plurality of user interactions, with a predetermined behavior,” referred to in

Wright as a “behavioral gene.” *Id.* ¶ 7. Wright describes the following example:

For example, a behavioral gene called “Internet download” may be created and stored in association with the computer network. This behavioral gene may summarize the user behaviors of 1) executing a hyperlink on the Internet, and 2) performing a “save as” action in which a file is saved to a location in the computer network, such as a hard drive. A single user behavior (e.g., closing an application) may be recorded and stored as a behavioral gene. Alternatively, a plurality of user behaviors may be recorded within a single behavioral gene.

Id. Similarly, “the indication of the code operation may be a result of comparing an operation with a predetermined code behavior,” referred to in Wright as a “code gene.” *Id.* ¶ 8. Examples of code genes are a “virus definition,” “malware definition,” and “adware definition.” *Id.* Wright discloses that “[a] combination of one or more behavioral genes may be combined with one or more code genes and the combination compared to a predetermined collection of user behavior-code operation indications,” referred to in Wright as “phenotypes.” *Id.* A phenotype is a “grouping of specific behavioral and code gene combinations that are typically present in a type of malicious usage session or operation with a computer.” *Id.* ¶¶ 8, 89. When the system identifies a phenotype, it may cause a particular remedial action to occur, such as an “intrusion preventive action.” *Id.* ¶¶ 8–9, 89.

Figure 4 of Wright is reproduced below.

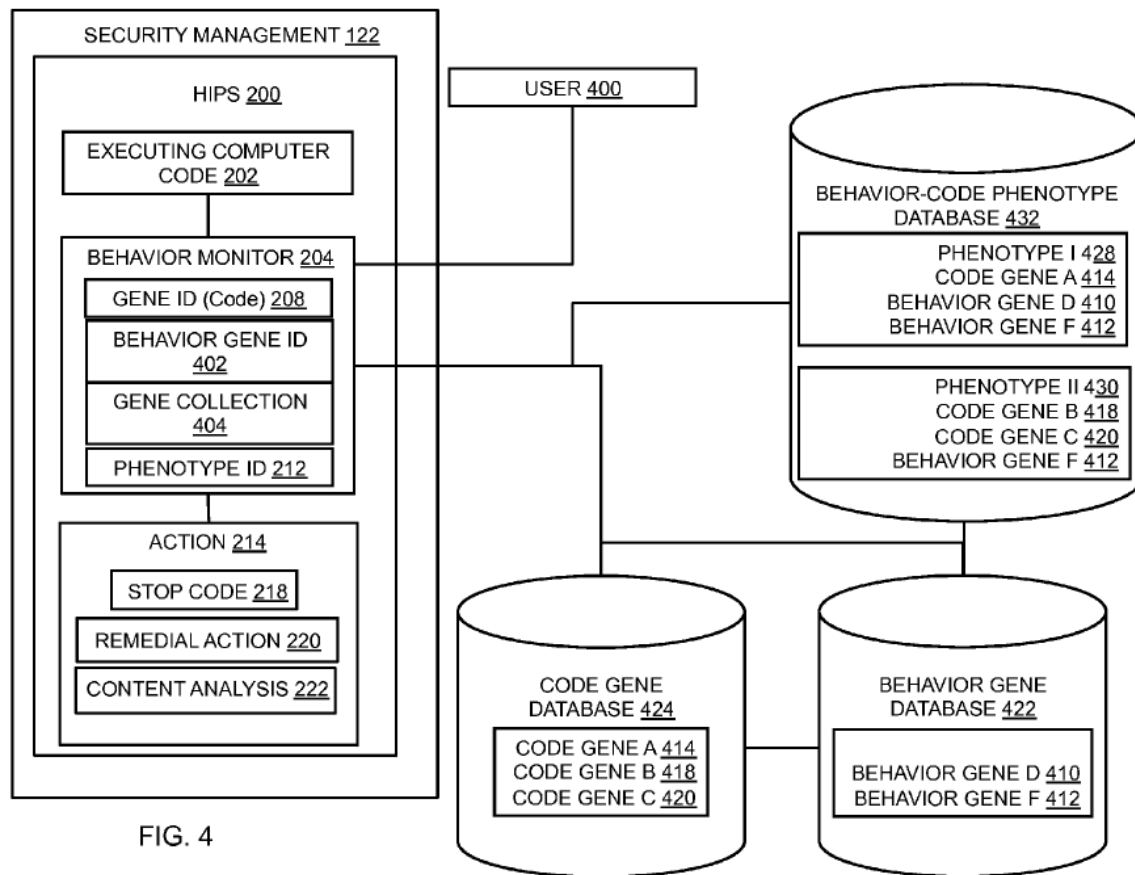


Figure 4 depicts the disclosed system comprising host intrusion prevention system (HIPS) 200 with behavior monitor facility 204 that “guard[s] against unknown threats by analyzing the behavior of a user 400 and the behavior at runtime for executing software code 202.” *Id.* ¶ 82. Behavior monitor facility 204 compares one or more behaviors of user 400 with a “predetermined behavior gene” stored in behavior gene database 422, compares operation of the executing code with a “predetermined code gene” stored in code gene database 424, collects a combination of behavioral and code genes, and compares the collection to identify a behavior-code phenotype stored in behavior-code phenotype database 432. *Id.* ¶¶ 84–88. Wright discloses that “[b]ehavior-code phenotypes may capture a combination or a series of user and code 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.” *Id.* ¶ 89. Phenotypes “may be created based on suspicious or risky user behavior . . . and scaled analysis of families of malware in runtime.” *Id.*

2. *Daswani*

Daswani discloses a method of “behavioral scanning of mobile applications for malware.” Ex. 1006, col. 1, ll. 59–60. Mobile devices download applications, which may or may not contain malware, from an application server. *Id.* at col. 3, ll. 29–35. A behavioral analysis server analyzes an application for malware by installing the application and running it on “software emulating the operating system of the mobile device.” *Id.* at col. 3, ll. 57–66. The server “place[s] an emulated mobile device in various states through simulated user interactions” and classifies behaviors as “hard signals” or “soft signals” indicating the likelihood that the behavior is “due to malware on the application being tested.” *Id.* at col. 2, ll. 59–61, col. 3, l. 66–col. 4, l. 5, col. 5, ll. 43–52. “[S]oft signals comprise system calls or actions which have an associated probability of the application containing malware.” *Id.* at col. 6, ll. 49–51. “For example, a soft signal may be accessing an address book on the mobile device. This action may be used for malicious purposes, but is often benign.” *Id.* at col. 6, ll. 55–58. The soft signal of accessing an address book can be “assigned an increased probability of maliciousness based on the amount of address book entries accessed or the pattern in which entries are accessed.” *Id.* at col. 6, ll. 60–63. “Hard signals comprise system calls or actions that are by definition malicious actions, or associated with a probability of the

application containing malware, the probability exceeding a hard signal threshold.” *Id.* at col. 6, ll. 52–55. For example, “[c]ontacting an internet protocol (IP) address associated with a known malicious botmaster may be classified as a hard signal due to the small probability of benign software performing such an action.” *Id.* at col. 6, l. 66–col. 7, l. 2.

Daswani discloses an equation $X = (D * P) / (D * P + F * (1 - P))$ for calculating “the probability of maliciousness, X, that an application is malicious when a single independent soft signal is observed,” where

P is the overall probability that any application contains malware without specific information about the application, D is the detection rate or probability that the soft signal is observed for a malicious application, and F is the false positive rate or probability that the soft signal is observed for a legitimate application.

Id. at col. 7, ll. 9–23. “The equation indicates that both the detection rate and false positive rate of observed soft signals are taken into account.

A signal with a high detection rate and a low false positive rate increases the probability of maliciousness when the signal is observed.” *Id.* at col. 7,

ll. 24–28. Daswani further discloses “combining hard signals and soft signals to determine a likelihood of malware” by determining hard signal behaviors and calculating a probability of maliciousness for each, determining soft signal behaviors and calculating a probability of maliciousness for each, combining the probabilities for the soft signals to determine a “combined probability of maliciousness,” and either

(1) classifying the application as malicious if a hard signal is observed or if the combined probability exceeds a “maliciousness threshold,” or
(2) classifying the application as non-malicious if no hard signals are

observed and the combined probability does not exceed the threshold. *Id.* at col. 8, ll. 3–27, Fig. 5.

3. *Claim 1*

Petitioner argues that Wright and Daswani collectively teach all of the limitations of claim 1. Pet. 9–39. With respect to the preamble of claim 1, Petitioner argues that Wright teaches a “method for assessing runtime risk for an application program that executes on a device” because “Wright’s system detects sequences of behaviors that correspond to risky or dangerous processes and then groups behaviors to identify malware.” *Id.* at 17–18 (citing Ex. 1005 ¶¶ 7, 66).² Patent Owner does not dispute Petitioner’s arguments regarding the preamble of claim 1. Regardless of whether the preamble of claim 1 is limiting, Petitioner shows sufficiently for purposes of institution that Wright teaches the preamble.

Limitation 1[b] recites “storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence,” and limitation 1[f] recites that “the action sequence is a sequence of at least two performed actions” and “each performed action is at least one of: a user action, an application action, and a system action.” Petitioner argues that Wright’s behavioral and code genes are both “rules” stored in a “rules database” (i.e., databases 422 and 424 shown in Figure 4), and the user interactions and code operations identified by the genes constitute “action sequence[s]” of

² We note that some citations to Wright in the Petition appear to be incorrect, as they refer to column and line numbers rather than paragraph numbers. *See, e.g.*, Pet. 17–18, 20, 23, 25, 29, 32–33. Although we are able to determine the correct paragraphs by searching for the quoted material, the parties should refer to Wright solely by paragraph number in future papers.

“at least two performed actions.” *Id.* at 18–19, 22–23, 37–38. Regarding user interactions, Petitioner notes that Wright describes comparing a plurality of user interactions to a “predetermined behavior” (i.e., a “behavioral gene”) and discloses a specific example of an “Internet download” behavioral gene with two user behaviors. *Id.* at 20–22 (citing Ex. 1005 ¶¶ 7, 75). Regarding code operations, Petitioner cites Wright’s description of various exemplary operations, such as “system startup, login, [a] scheduled job process, [and] system service,” and argues that a person of ordinary skill in the art would have known that such operations “include multiple ‘system actions’ including, at least, system file creation, system folder modification, registry modification or additions, application setting modifications, driver install or uninstall, network activity, execution from temporary system files, and so forth.” *Id.* at 23–25 (quoting Ex. 1005 ¶ 13; citing Ex. 1003 ¶¶ 63–69).

Patent Owner makes three arguments in response. First, Patent Owner contends that “Wright only mentions ‘rules’ in the context of providing access permissions” and the disclosed rules for granting access to a resource do not identify an action sequence. Prelim. Resp. 15 (citing Ex. 1005 ¶ 35). Patent Owner is correct that Wright uses the term “rules” in one paragraph pertaining to access rights, but that does not address Petitioner’s argument in the Petition—namely, that Wright’s genes constitute “rules” as recited in claim 1. *See Adasa Inc. v. Avery Dennison Corp.*, 55 F.4th 900, 910 (Fed. Cir. 2022) (a prior art “reference need not disclose the elements in the very same terms used by the patent,” as “[t]he reference need not satisfy an *ipsissimis verbis* test”).

Second, Patent Owner argues that Wright’s behavioral and code genes “are, at most, actions or events,” not “rules,” “because Wright’s databases

aggregate predetermined user behaviors or code behaviors.” *Id.* at 15–16 (citing Ex. 1005 ¶¶ 7–8). We disagree on this record. As shown in Figure 4, the entries in behavior and code gene databases 422 and 424 are genes (identified as 410, 412, 414, 418, and 420), not individual behaviors, and, at least in the case of behavioral genes, Wright expressly states that a behavioral gene can comprise multiple behaviors. *See* Ex. 1005 ¶¶ 7 (describing the “Internet download” behavioral gene having two behaviors and stating that “[a] single user behavior (e.g., closing an application) may be recorded and stored as a behavioral gene. Alternatively, a *plurality of user behaviors* may be recorded within a single behavioral gene.” (emphasis added)), 75 (same), 84–87 (“comparing one or more user 400 behaviors with a predetermined behavior gene”), Fig. 4; Pet. 18, 21–22, 37–38 (“user behavior monitored in Wright can include a sequence of user interactions”).

Third, Patent Owner argues that Petitioner “improperly conflates Wright’s ‘genes’ with both the claimed ‘action sequences’ and the claimed ‘rules,’” thereby “render[ing] the claim language that ‘each rule identifies an action sequence’ redundant because an action sequence cannot identify itself.” Prelim. Resp. 16–17. Petitioner, however, maps Wright’s behavioral and code genes to the “rules” of claim 1 and maps a plurality of actions, such as user behaviors, for a gene to the recited “action sequence” that a rule identifies. Pet. 18–25, 37–38. Thus, we do not agree on this record that Petitioner improperly maps the same thing in Wright to both claim limitations.

Next, we turn to limitations 1[c] and 1[d]. With respect to limitation 1[c], “storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules,” Petitioner argues that Wright’s phenotypes are “assessment policies”

stored in a “policy database” (i.e., database 432 shown in Figure 4), where each phenotype includes at least one behavioral gene and at least one code gene (both of which are “rules”). *Id.* at 25–27 (citing Ex. 1005 ¶ 8).

According to Petitioner, “Wright discloses that different phenotypes are associated with suspicious behaviors, different phenotypes can be compared against the runtime object’s behavior, and a confidence level can be associated with each of the different phenotypes.” *Id.* at 26–27.

With respect to limitation 1[d], “identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application,” Petitioner argues that “behavior monitoring facility 204 in Wright uses phenotypes ([each an] ‘assessment policy’) to analyze runtime behavior [of] an application program that executes on a device, in which the runtime behavior indicates a risk or threat of the identified user behavior and code behavior (each an ‘action sequence’).” *Id.* at 28–29. According to Petitioner, Wright identifies a “runtime risk” “based on the connection between a recognized phenotype and a known family of malware.” *Id.* at 30. Petitioner argues that Wright “ranks phenotypes according to their relationship to known families of malware,” and a person of ordinary skill in the art “would recognize an identification of a known family of malware to be a ‘risk or threat of the identified action sequence’” as recited in claim 1. *Id.* at 30–31.

Patent Owner responds that “Wright’s phenotypes are simply collections of stored genes that have some commonality” and, “[a]s a mere collection of behaviors, each phenotype cannot be an assessment policy because a collection of behaviors (*i.e.*, phenotype) cannot perform an assessment of risk, let alone ‘a runtime risk’ as the subsequent [limitation

1[d]] requires.” Prelim. Resp. 17–18 (citing Ex. 1005 ¶¶ 8, 69). In Patent Owner’s view, “Wright’s phenotypes do not perform any assessment of *runtime* risk because each phenotype is already *predetermined* to be associated with a known family of malware.” *Id.* at 18 (citing Ex. 1005 ¶ 69).

We do not see on this record, however, why Wright’s comparison of monitored actions to phenotypes stored in memory fails to teach the recited identification of a runtime risk. As Petitioner points out, Wright performs the comparison at runtime and determines the occurrence of a particular phenotype. *See* Pet. 26–29; Ex. 1005 ¶ 82 (“[B]ehavior monitoring facility 204 may guard against unknown threats by analyzing the behavior of a user 400 and the behavior at runtime for executing software code 202.”). Wright also identifies the extent of the connection between the behaviors for a particular phenotype and a known family of malware, ranking the phenotypes according to that level of connection. *See* Pet. 30–31. Wright discloses:

Phenotypes 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*. The predetermined collections of behaviors, or phenotypes, may be created based on scaled analysis of families of malware in runtime, such as in a threat research facility 132 of a threat management facility 100. Including greater combinations of behaviors in the phenotype database 224 may enable more detailed analysis of a suspicious code. For example, an analysis of a suspicious code may be moved from ‘Accessing the registry in this location is bad’ to ‘This process is exhibiting the same behavior as the family of malware Conficker’ based on a comparison of a detected phenotype with an existing phenotype.

Ex. 1005 ¶ 69 (emphasis added); *see also id.* ¶ 89 (“Behavior-code phenotypes may capture a combination or a series of user and code 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.”). Petitioner has shown sufficiently at this stage that when Wright’s system performs the comparison and determines that a sequence of monitored actions corresponds to one of the stored phenotypes, Wright identifies, using an “assessment policy” (i.e., a phenotype) a runtime risk that “indicates a risk or threat of the identified action sequence of the application” (i.e., a risk that the monitored actions are indicative of malware within the known family of malware). *See* Pet. 30–31.

Patent Owner also attempts to distinguish Wright by pointing to the statement in the Specification of the ’517 patent that an assessment policy “may identify the runtime risk based on matching rules and probabilistic weights and scores” and arguing that Wright by contrast “only uses comparisons of previously stored actions to runtime behaviors to determine threats or malware.” Prelim. Resp. 20 (quoting Ex. 1001, col. 6, ll. 14–19). Limitation 1[d], however, only recites that the identifying step “us[es] at least one assessment policy.” It does not further recite *how* the identification is performed and does not, for example, require using “matching rules” or “probabilistic weights and scores” as described for the exemplary embodiment in the Specification.³

³ To the extent the parties disagree as to the interpretation of “rules,” “assessment policy,” “runtime risk,” “behavior score,” or any other terms of the challenged claims, the parties are encouraged to provide in their papers during trial proposed interpretations for the term(s) and cite support in the Specification and/or prosecution history of the ’517 patent for their respective interpretations.

With respect to limitation 1[e], “identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk,” Petitioner argues that Wright’s behavior monitoring facility 204 with a processor constitutes a “runtime monitor including a processing device.” Pet. 31–33. Petitioner further contends that behavior monitoring facility 204 identifies a behavior score because “Wright discloses a ranking system for which a [person of ordinary skill in the art] would understand that a ‘score’ is the basis for the ranking probability that the monitored software code (corresponding to the application program that executes on the device) is malware, and thus presenting a risk or threat.” *Id.* at 33–34 (citing Ex. 1005 ¶ 69); *see* Ex. 1003 ¶¶ 166–169.

Patent Owner responds that Petitioner fails to show that “Wright’s ‘rankings’ are *based on* Wright’s ‘identification of a known family of malware’” because the phenotypes are ranked prior to identifying the appropriate family of malware at runtime. Prelim. Resp. 21–22. At this stage, we question whether Wright alone teaches or suggests the “behavior score” aspect of limitation 1[e]. Petitioner’s position is that a person of ordinary skill in the art would have understood Wright to teach a “score,” but Wright does not expressly disclose such a score—just rankings—and the only supporting evidence cited is Wright’s teaching of ranking phenotypes in advance. *See* Pet. 33–34; Ex. 1003 ¶¶ 166–169.

Petitioner, however, makes an alternative argument relying on the combined teachings of Wright and Daswani that we find persuasive based on the current record. Pet. 34–36. Petitioner contends that “[w]hile Wright indicates that the combination or series of behaviors will be ranked to create increasing levels of confidence that an application is malware, Daswani

discloses a probabilistic scoring to determine an overall likelihood that an application is malicious, and thus poses a threat to the system.” *Id.* at 34. Petitioner relies on Daswani’s teachings of “hard and soft signals that represent indications of how much a system call or action is likely to contain malware, a significant indicator of risk,” modeling behaviors as signals, and calculating a value called the “probability of maliciousness,” or “X,” based on a set of observed signals. *Id.* at 34–36 (citing Ex. 1006, code (57), col. 6, ll. 47–55, col. 7, ll. 9–20). According to Petitioner and Dr. Nielson, a person of ordinary skill in the art would have understood the calculated probability of maliciousness to be a “behavior score.” *Id.* at 36 (citing Ex. 1003 ¶ 174). Petitioner also provides an explanation for why an ordinarily skilled artisan would have been motivated to “use Daswani’s approach in Wright’s system.” *Id.* at 12–17; *see* Ex. 1003 ¶¶ 103–115. For example, Petitioner argues that Wright ranks phenotypes “based on confidence,” Daswani “discloses how to create these confidence levels,” and using Daswani’s method would maximize classification flexibility while minimizing false positives. Pet. 12–16.

Patent Owner argues that “Petitioner does not explain how a [person of ordinary skill in the art] would identify Daswani’s ‘calculated probability of maliciousness’ *based on* Wright’s ‘identification of a known family of malware,’” as Daswani’s probabilities of maliciousness are calculated based on hard and soft signals “*prior to* classifying an application as malicious.” Prelim. Resp. 23–24 (citing Ex. 1006, col. 8, ll. 13–27). We disagree based on the current record. As explained above in connection with limitation 1[d], we are persuaded on this record that Wright identifies a runtime risk by monitoring actions at runtime and determining that a pattern of actions matches a stored phenotype, where the phenotype has a recognized

connection to a known family of malware and is ranked in comparison to other phenotypes that may indicate the presence of malware with different levels of confidence. *See* Pet. 28–31. Daswani discloses a specific method of scoring such confidence levels (i.e., calculating a probability of maliciousness). *See id.* at 34–36; Ex. 1006, col. 7, ll. 9–28. Daswani’s calculated probability of maliciousness is based on observed soft signals that occur at runtime, similar to Wright’s determination of a particular phenotype based on observed behaviors occurring at runtime. *See* Ex. 1005 ¶¶ 82–88; Ex. 1006, col. 8, ll. 6–16. Petitioner’s asserted combination is to use Daswani’s calculated probability of maliciousness (i.e., a “behavior score” in Petitioner’s view) in Wright’s system as a numerical measure of the connection to the known family of malware, and Petitioner provides sufficient explanation at this stage as to why doing so would have been advantageous. *See* Pet. 12–17, 34–36.

Petitioner’s contentions regarding claim 1 are supported by the testimony of Dr. Nielson and are persuasive based on the current record. *See* Pet. 9–39; Ex. 1003 ¶¶ 102–192. Petitioner has made a sufficient showing on this record that Wright and Daswani collectively teach all of the limitations of claim 1 and that a person of ordinary skill in the art would have been motivated to modify Wright’s system, based on the teachings of Daswani, to identify a behavior score, with a reasonable expectation of success in doing so to achieve the claimed method. We are persuaded that Petitioner has shown a reasonable likelihood of prevailing on its assertion that claim 1 is unpatentable over Wright and Daswani. Accordingly, we institute review “on all of the challenged claims and on all grounds of unpatentability asserted for each claim.” *See* 37 C.F.R. § 42.108(a).

4. *Claims 2–24*

Independent claim 13 is similar to claim 1, reciting a “rules database storing a plurality of rules,” a “policy database storing a plurality of assessment policies,” and a “runtime monitor including a processing device” that performs the same two “identifying” steps recited in claim 1.

Petitioner’s analysis of claim 13 relies on much of its earlier analysis of claim 1. Pet. 59–61; *see* Ex. 1003 ¶¶ 268–288. Patent Owner only makes arguments as to claim 1 in its Preliminary Response. Prelim. Resp. 24.

On this record, we are persuaded that Petitioner has shown a reasonable likelihood of prevailing on its assertion that claim 13 is unpatentable over Wright and Daswani, and need not determine at this time whether Petitioner also has shown a reasonable likelihood of prevailing as to any of dependent claims 2–12 and 14–24. *See* 37 C.F.R. § 42.108(a).

III. CONCLUSION

Based on the arguments presented in the Petition, we conclude that Petitioner has demonstrated a reasonable likelihood of prevailing with respect to at least one claim of the ’517 patent challenged in the Petition. Accordingly, we institute a trial on all claims and all grounds asserted in the Petition. The Board has not made a final determination under 35 U.S.C. § 318(a) with respect to the patentability of the challenged claims.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–24 of the ’517 patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the ’517 patent shall commence on the entry date of this Decision, and notice is hereby given of the institution of a trial.

IPR2023-00798
Patent 8,850,517 B2

FOR PETITIONER:

Robert M. Hansen
Scott B. Amankwatia
THE MARBURY LAW GROUP, PLLC
bhansen@marburylaw.com
samankwatia@marburylaw.com

FOR PATENT OWNER:

Peter Lambrianakos
Vincent J. Rubino, III
Joseph M. Mercadante
FABRICANT LLP
plambrianakos@fabricantllp.com
vrubino@fabricantllp.com
jmercadante@fabricantllp.com