UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/201,171	07/01/2016	Philipp Reinecke	90214803	7524

146568 7590 03/23/2020

MICRO FOCUS LLC
500 Westover Drive
#12603
Sanford, NC 27330

EXAMINER
JACKSON, JENISE E

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
03/23/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

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

software.ip.mail@microfocus.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte PHILIPP REINECKE, MARCO CASASSA MONT, and YOLANTA BERESNA

Appeal 2019-005645
Application 15/201,171
Technology Center 2400

Before MICHAEL J. STRAUSS, JAMES B. ARPIN, and AMBER L. HAGY, *Administrative Patent Judges*.

ARPIN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a) the final rejection of claims 1–20, all of the pending claims. Final Act. 2.[2] We have jurisdiction under 35 U.S.C. § 6(b).

---

[1] "Appellant" here refers to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party-in-interest as EntIT Software LLC, a subsidiary of Micro Focus International Plc. Appeal Br. 3.

[2] In this Decision, we refer to Appellant's Appeal Brief ("Appeal Br.," filed October 15, 2018) and Reply Brief ("Reply Br.," filed July 15, 2019); the Final Office Action ("Final Act.," mailed June 15, 2018) and the Examiner's Answer ("Ans.," mailed May 15, 2019); and the originally-filed Specification ("Spec.," filed July 1, 2016). Rather than repeat the Examiner's findings and determinations and Appellant's contentions in their entirety, we refer to these documents.

We affirm-in-part, and we enter a new ground of rejection with respect to claim 1 under 35 U.S.C. § 101.

STATEMENT OF THE CASE

Appellant's claimed subject matter relates to "devices and methods . . . used to identify computer attacks at various stages, e.g., using symptoms or signatures of known attacks." Spec. ¶ 1. In particular,

> [c]omputer attack models may be used to drive detection, tracking, and prediction of malware and other malicious attacks on a computing system. The behavior of attacks on computer systems, whether a single computer or a large network of many computing devices, can be modeled at a high level. For example, the high level behavior of a data exfiltration attack - where an attack attempts an unauthorized export of some type of data from a computing system - can be modeled in a way that captures most data exfiltration attacks. E.g., such an attack may begin with an infection phase, followed by a discovery phase, then a lateral movement phase, and finally a data exfiltration phase. *An attack model may include a variety of information that describes potential actions that could be taken in any given phase, or state, of an attack.*"

Id. ¶ 8 (emphasis added). Referring to Figure 2, the Specification explains

> [t]he example attack model specifies, for each of four phases, attack actions that may occur during a data exfiltration attack, e.g., an attack designed to transfer data from a target computing system. Phase 1 202, the infection phase, specifies three actions that may occur when an attack tries to infect a computing system: i) install remote access Trojan (RAT), ii) establish a control channel, and iii) ongoing command and control communication.

Id. ¶ 17.

As noted above, claims 1–20 stand rejected. Claims 1, 8, and 15 are independent. Appeal Br. 26 (claim 1), 28 (claim 8), 30 (claim 15) (Claims App.). Claims 2–7 depend directly or indirectly from claim 1, claims 9–14

depend directly or indirectly from claim 8, and claims 16–20 depend directly from claim 15. *Id*. at 26–31.

Claims 1–3, reproduced below with disputed elements emphasized, are representative.

> 1. A computing device for computer attack model management, the computing device comprising:
>
> a hardware processor; and
>
> a data storage device storing instructions that, when executed by the hardware processor, cause the hardware processor to:
>
> identify a first set of attack models, wherein a computing system is susceptible to a particular attack on the computing system *and each attack model in the first set of attack models specifies a behavior of the particular attack on the computing system*;
>
> obtain, for each attack model in the first set, *performance data that indicates at least one measure of attack model performance for a previous use of the attack model in determining whether the particular attack occurred on the computing system*; and
>
> *update the first set of attack models based on the performance data to add an attack model to the first set of attack models or remove an attack model from the first set of attack models*.
>
> 2. The computing device of claim 1, wherein the performance data includes at least one of:
>
> *resource usage measurements that indicate computing resources used to execute actions specified by the corresponding attack model*; or
>
> analytics results data that indicates a frequency with which the corresponding attack model successfully detected the particular attack.
>
> 3. The computing device of claim 1, wherein the instructions, when executed by the hardware processor, cause the

> hardware processor to update the first set of attack models *in response to a triggering event*.

Id. at 26 (emphases added). Independent claims 8 and 15 recite limitations corresponding to the disputed limitations of claims 1–3 (*id.* at 28, 30).

REFERENCES AND REJECTIONS

The Examiner relies upon the following references in rejecting the claims:

Name[3]	Number	Publ'd/Issued	Filed
Di Pietro	US 2016/0028750 A1	Jan. 28, 2016	July 23, 2014
Yen	US 9,378,361 B1	June 28, 2016	Dec. 31, 2012
Lin	US 2017/0228659 A1	Aug. 10, 2017	Mar. 28, 2016

Specifically, the Examiner rejects claims 1–13, 15–17, 19, and 20 under 35 U.S.C. § 103 as obvious over the combined teachings of Di Pietro and Yen (Final Act. 10–16); and claims 14 and 18 under 35 U.S.C. § 103 as obvious over the combined teachings of Di Pietro, Yen, and Lin (*id.* at 16–17).[4]

Appellant contests the obviousness rejection of independent claims 1, 8, and 15 (Appeal Br. 13–19), and relies on similar deficiencies in the rejection of each independent claim to overcome the rejections of dependent claims 4–6, 9–11, 14, and 17–19 (*id.* at 24–25). Appellant contests separately the rejection of dependent claims 2, 3, 7, 12, 13, 16, and 20. *Id.* at 20–24. Because we determine that affirmance of the rejection of the

[3] All reference citations are to the first named inventor only.

[4] The Examiner rejected claims 1–20 as directed to an abstract idea without significantly more (Final Act. 7–9), but withdrew that rejection (Ans. 3).

independent claims is dispositive, except for our ultimate decision, we do not discuss the merits of the rejections of claims 4–6, 9–11, 17, and 19 further herein. We address separately Appellant's contentions with respect to claims 2, 3, 7, 12–14, 16, 18, and 20.

We review the appealed rejections of the claims for error based upon the issues identified by Appellant, and in light of the arguments and evidence produced thereon. *Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential). Arguments not made are waived. *See* 37 C.F.R. § 41.37(c)(1)(iv). Unless otherwise indicated, we adopt the Examiner's findings in the Final Action and the Answer with respect to the affirmed rejections as our own and add any additional findings of fact for emphasis. We address the rejections of the separately argued claims below.

ANALYSIS

1. Obviousness Over Di Pietro and Yen

a. Independent Claim 1

The Examiner finds that Di Pietro teaches or suggests almost all of the limitations of independent claim 1. Final Act. 10–11. The Examiner finds, however, that, although Di Pietro teaches or suggests an attack model (*id.* at 11 (citing Di Pietro, Fig. 9 (step 915: "PROVIDE [EXPECTED TRAFFIC] MODEL TO NODE(S)")); *see* Di Pietro ¶ 75; *see also* Spec. ¶¶ 8, 17 (defining an "attack model")), "Di Pietro does not explicitly disclose a first set of attack models" (Final Act. 11).

Nevertheless, the Examiner finds that Yen teaches or suggests a first set of attack models. *Id.* (citing Yen, 3:40–46, 4:27–31, 5:38–41). In particular, the Examiner finds Yen discloses building a plurality of templates. Yen explains,

> [t]he major component of the threat detection system 18 is the monitor/analyzer 22. As described more below, it employs both top-down and bottom-up components. *The top-down component builds and utilizes templates based on known information about current and prior [advanced persistent threats (APT)] attacks, and these templates are used in analysis for detecting behavior that may be indicative of such attacks.*

Yen, 3:40–46 (emphasis added). Further, Yen explains,

> *[s]tarting from the general APT model, different classes of attacks can be defined and the classes used to guide template creation.* Examples of attack classes include attackers that propagate through social media, attackers that gather data to a central location and exfiltrate the data, attackers that exfiltrate from multiple machines in the enterprise. *Templates for such different classes of attack can be built and deployed for use.* The templates can also be refined during use as more knowledge is gathered about attacker behavior.

Id. at 4:22–30 (emphases added); *cf.* Spec. ¶ 17 (describing "data exfiltration attack").

Yen teaches, "[a] framework is used in which templates are defined by a human analyst for the correlations implemented by the correlators." Yen, 2:29–31. Di Pietro similarly teaches the following:

> In some aspects, the update to the classifier may leverage the recommendation of an external expert, such as a network administrator, etc. On one hand, the techniques herein may improve the reliability of a learning machine-based attack detection mechanism, such as when [a machine learning classifier (e.g., an Artificial Neural Networks (ANN))] is used.

Di Pietro ¶ 52; *cf.* Spec. ¶ 24 (describing "user feedback"). The Examiner concludes that a person of ordinary skill in the relevant art would have had reason to combine the teachings of Di Pietro and Yen to modify the teachings of Di Pietro to include a first set of attack models, as taught by Yen. Final Act. 11.

Appellant contends that the Examiner erred in rejecting claim 1 for at least four reasons. Appeal Br. 13–17. For the reasons given below, we disagree.

First, Appellant contends, "neither Di Pietro's traffic model nor its attack detector/classifier may be considered the attack model of claim 1." *Id.* at 15. In particular, Appellant contends

> Di Pietro discusses an expected traffic model (See, for example, paragraph number [0045] of Di Pietro) and an attack detection classifier. As explained in paragraph number [0018] of Di Pietro, "according to one or more embodiments of the disclosure, a device in a network generates an expected traffic model based on a trained set of data used to train a machine learning attack detector."
>
> In paragraph number [0068], Di Pietro discusses evaluating the performance of the attack detector, or classifier, and based on the performance, the expected traffic model may be updated (if the performance of the classifier is "tolerable"), or "otherwise, if the current version of the attack detector is unable to satisfy the required performance, [signature generation process (SGE)] 402 may also update the attack 14 detector by adding the traffic samples to the training data set for the relevant class and recomputing the attack detector." Di Pietro, para. no. [0068].

Appeal Br. 14–15.

Initially, we note that the Specification defines "attack model" broadly. In particular, the Specification states, "[a]n attack model may include a variety of information that describes potential actions that could be taken [by an attacker] in any given phase, or state, of an attack." Spec. ¶ 8; *see id.* ¶ 17. We interpret "attack model" accordingly.

In response to Appellant's contentions, the Examiner finds Di Pietro teaches that a machine learning attack detector is updated, so that it is able to

recognize observed traffic behavior as an attack if the traffic behavior occurs again. Ans. 4 (citing Di Pietro ¶ 53). Further, observing particular traffic behavior, the attack detector may label the observed traffic behavior as an attack. *Id.* (citing Di Pietro ¶ 48); *see* Di Pietro ¶¶ 71, 72 (describing automatic assessment of unexpected behavior and distinguishing between "normal traffic" and "a new attack class"). We agree with the Examiner. Therefore, we disagree that Di Pietro's traffic model or its attack detector/classifier fails to teach or suggest the attack model of claim 1.

Second, Appellant contends:

> Claim 1 recites, "each attack model in the first set of attack models specifies the particular attack on the computing system" (emphasis added). Di Pietro fails to disclose or render obvious updating a set of attack detectors, where each detector specifies behavior of *the same particular attack* on a computer system based on performance data that indicates measure(s) of attack model performance use of the attack model in determining whether the particular attack occurred.

Appeal Br. 16 (italics added); *see* Reply Br. 1–2. As the Specification explains, however, *"[i]n some implementations*, each model in the first set is for *the same type* of computer attack." Spec. ¶ 23 (emphases added).

The Examiner finds Appellant improperly reads limitations from the Specification into the claims. Ans. 6. The term: "*the* particular attack" takes antecedent basis from the term: "*a* particular attack," which we interpret to mean one or more particular attacks. *E.g.*, Spec. ¶¶ 8 ("The behavior of attacks on computer systems, whether a single computer or a large network of many computing devices, can be modeled at a high level. For example, the high level behavior of a data exfiltration attack - where an attack attempts an unauthorized export of some type of data from a computing system - can be modeled in a way that captures most data exfiltration

attacks."), 21 ("Other data exfiltration attack models, aside from the example data exfiltration attack model 200, may be used for data exfiltration attacks. Other data exfiltration attack models may specify different attack actions and/or different phases; attack models need not include all actions or phases of a given attack. In addition, attack models may exist for many different types of attacks, such as [distributed denial of service (DDOS)][5] attacks, attacks designed to destroy rather than export data, ransomware attacks, etc."); *see Harari v. Lee*, 656 F.3d 1331, 1341 (Fed. Cir. 2011); *Baldwin Graphic Systems, Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342–43 (Fed. Cir. 2008). Because we agree with the Examiner that Appellant's contentions are not based on the language of claim 1, we do not find those contentions persuasive of error.

Third, Appellant contends, "Di Petro fails to disclose or render obvious updating a first set of attack models based on performance data by adding an attack model to or removing an attack model from the first set of attack models," and Yen fails to cure this deficiency. Appeal Br. 16–17. In particular, Appellant contends

> Yen fails to disclose or render obvious updating a first set of attack models based on performance data (which indicates at least a measure of an attack model performance from previous use in the attack model in determining whether *the same particular attack* occurred on the computing system), regardless of whether Yen is considered singularly or in combination with Di Pietro.

Id. at 17 (emphasis added). We disagree.

Initially, we note Appellant relies on the same inaccurate characterization of the language of claim 1 as in its previous contention. *See*

[5] *See* Di Pietro ¶ 3 ("a distributed DoS (DDoS) attack").

Ans. 6, 7–8. Further, the Examiner relies on Di Pietro, not Yen, to teach the "update" limitation of claim 1. *Id.* at 8–9; *see* Final Act. 11.

Di Pietro discloses:

> When a new attack type is identified by ground truth 606, SGE 402 may create a new attack class and add the observed traffic samples exhibiting the unexpected behavior to the training data set for the attack classifier, with a correct label identifying the new attack. SGE 402 may then update the attack detector using the updated training data set and the new classification. For example, the entire ANN classifier or a portion thereof may be recomputed using the updated training data. *Subsequently, SGE 402 may then send an updated version of the attack detector that can now recognize the new attack to any or all of the nodes/devices 104.* In addition, SGE 402 may generate and send an updated expected traffic model that incorporates the previously unexpected behavior into the training data set.

Di Pietro ¶ 67 (emphasis added); *see id.* ¶ 93. The Specification defines "performance data" broadly, explaining that

> the performance data 152 includes resource usage measurements, analytics results data, and/or user feedback. *The resource usage measurements may indicate the computing resources used to execute analytics for actions specified by the corresponding attack model, e.g., number and usage rate of data processors, volatile memory usage, long-term memory usage, computing time, personnel involvement time, etc.* The analytics results data may indicate whether the corresponding attack model successfully detected the particular attack, e.g., the frequency with which attack action detection was successful, how many devices the attack actions were confirmed on, the time it took to confirm an attack action occurred and/or the entire attack occurred.

Spec. ¶ 24 (emphasis added). In view of this broad definition of performance data, we are persuaded the Examiner has shown Di Pietro, in combination with Yen, teaches or suggests "instructions that . . . update the

first set of attack models based on the performance data to add an attack model to the first set of attack models or remove an attack model from the first set of attack models." Final Act. 11; Ans. 6–7; *see* Appeal Br. 26 (Claims App.) (quoting claim 1).

Fourth, Appellant contends Examiner relies on improper hindsight in combining the teachings of Di Pietro and Yen to achieve the device of claim 1. Appeal Br. 17.

> Any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning, but so long as it takes into account only knowledge which was within the level of ordinary skill [in the art] at the time the claimed invention was made and does not include knowledge gleaned only from applicant's disclosure, such a reconstruction is proper.

In re McLaughlin, 443 F.2d 1392, 1395, (CCPA 1971). Nevertheless, in view of the evidence supporting the Examiner's finding that a person of ordinary skill in the art would have had reason to combine the teachings of Di Pietro and Yen to achieve the recited device and Appellant's inaccurate characterization of the limitations of claim 1, we are not persuaded that the Examiner relied on improper hindsight in combining the teachings of Di Pietro and Yen to achieve the devices of claim 1. Final Act. 11.

We are not persuaded that the Examiner erred in the obviousness rejection of claim 1, and we sustain that rejection. Because the rejection of claims 4–6 is not contested separately, we also sustain that rejection.

b. Independent Claim 8

As with independent claim 1, the Examiner finds that Di Pietro teaches or suggests almost all of the limitations of independent claim 8. Final Act. 13–14. As with claim 1, the Examiner finds that, although

Di Pietro teaches or suggests an attack model, Yen teaches or suggests a first set of attack models (*id.* at 14 (citing Yen, 3:40–46)); and a person of ordinary skill in the art would have had reason to combine the teachings of Di Pietro and Yen to achieve the methods of claim 8 (*id.*).

Independent claim 8 recites limitations corresponding to the limitations discussed above with respect to claim 1. Appeal Br. 28 (Claims App.). Appellant raises substantially the same contentions regarding those limitations with respect to independent claim 8. *See* Appeal Br. 18–19. We are equally unpersuaded by these contentions with respect to the corresponding limitations of claim 8, as we are with respect to those of claim 1.

Nevertheless, claim 8 recites

> obtaining, for each attack model in the first set, performance data that indicates at least one measure of attack model performance for a previous use of the attack model in determining whether the particular attack occurred on the computing system, the performance data including:
>
> *resource usage measurements* that indicate computing resources used to execute actions specified by the corresponding attack model; and
>
> analytics results data that indicates whether the corresponding attack model successfully detected the particular attack; and
>
> *in response to a triggering event*, update the first set of attack models based on the performance data.

Appeal Br. 28 (Claims App.) (emphases added). Appellant contends the Examiner fails to show that Di Pietro teaches or suggests the recited "resource usage measurements" and "a triggering event" resulting in updates. For the reasons given below, we disagree.

First, Appellant contends "[c]laim 8 recites obtaining performance data that includes resource usage measurements that indicate computing resources that are used to execute actions that are specified by the corresponding attack model." Reply Br. 3. As noted above, we interpret the "*actions* that are specified by the corresponding attack model" to be actions of the attacker. Spec. ¶¶ 8, 17; *cf.* Yen 4:22–30.

Di Pietro discloses

> traffic behavior is observed by the node . . . . For example, the node may observe the number of requests, the bandwidth usage, the amount of delays, the amount of jitter, etc. of the traffic. In some cases, the behavior may be observed directly by the node (e.g., the traffic is flowing through the node itself). In other cases, the node may observe the traffic indirectly (e.g., by receiving traffic records from one or more other nodes in the network).

Di Pietro ¶ 91. Each of these behaviors is a measurement of resource usage resulting from the actions of an attacker. *See id.* ¶¶ 92–94. The Examiner finds that Di Pietro teaches or suggests "resource usage measurements," as recited in claim 8. Ans. 10–11. We agree.

Second, the Examiner finds that "Di Pietro discloses a triggering event, because Di Pietro discloses determin[ing] whether the observed traffic behavior is unexpected, the node may compare the observed traffic behavior to the expected traffic model, to determine whether or not the difference between the two exceeds *an anomaly threshold*." Ans. 11 (emphasis added). Appellant contends, "neither Di Pietro nor Yen discloses or renders obvious in response to a triggering event, updating a first set of attack models based on performance data." Appeal Br. 19; Reply Br. 3–4. In particular, Appellant contends:

> Even assuming, *arguendo*, that an "anomaly threshold" is used

> for the deviation determination, this still fails to disclose or render obvious the expressly-recited elements of claim 8. In this manner, Di Pietro states that the analytics results data indicates whether the corresponding attack model successfully detected the particular attack. In paragraph number [0092], Di Pietro discusses determining whether the observed traffic behavior is different from the behavior used to train the attack detector. Measurements pertaining to observed traffic behavior fails to disclose or render obvious measurements that indicate computing resources used to execute actions specified by an attack model.

Reply Br. 4. Thus, Appellant contends that Di Pietro does not teach or suggest the recited "triggering event" because Di Pietro's "anomaly threshold" is used for a different purpose.

Nevertheless, claim 8 recites "in response to a triggering event, updat[ing] *the first set of attack models* based on the performance data." Appeal Br. 28 (Claim App.) (emphasis added). Interpreting this limitation in view of the other claims and the Specification, we determine that to "update" may include "to add . . . or remove" an attack model to or from the first set of attack models. *See* Appeal Br. 26 (claim 1), 29 (claims 11, 12, 14), 30 (claim 15) (Claims App.); Spec. ¶ 25 ("In some implementations, the set of attack models is updated *by adding, removing, or changing* an attack model in the first set." (emphasis added)); *see Rexnord Corp. v. Laitram Corp.*, 274 F.3d 1336, 1342 (Fed. Cir. 2001); *In re Morris*, 127 F.3d 1048, 1053 (Fed. Cir. 1997); *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). Thus, we are persuaded the Examiner has adequately shown that Di Pietro teaches or suggests the "updat[ing]" limitation.

We are not persuaded that the Examiner erred in the obviousness rejection of claim 8, and we sustain that rejection. Because the rejection of claims 9–11 is not contested separately, we also sustain that rejection.

c. Independent Claim 15

As with independent claims 1 and 8, the Examiner finds that Di Pietro teaches or suggests almost all of the limitations of independent claim 15 Final Act. 16. As with claims 1 and 8, the Examiner finds that Yen teaches the missing limitations of claim 15, and a person of ordinary skill in the art would have had reason to combine the teachings of Di Pietro and Yen to achieve the computer-readable media storing instructions of claim 15. *Id.*

Independent claim 15 recites limitations corresponding to the limitations discussed above with respect to claims 1 and 8. Appeal Br. 30 (Claims App.). Appellant raises substantially the same contentions regarding those limitations with respect to independent claim 15. *See* Appeal Br. 19. We are equally unpersuaded by these contentions with respect to the corresponding limitations of claim 15, as we are with respect to those of claims 1 and 8.

For the reasons given above, we are not persuaded that the Examiner erred in the obviousness rejection of claim 15, and we sustain that rejection. Because the rejection of claims 17 and 19 is not contested separately, we also sustain that rejection.

d. Dependent Claims 2 and 16

In the devices of claim 1, claim 2 recites "the performance data includes at least one of: *resource usage measurements* that indicate computing resources used to execute actions specified by the corresponding attack model; or analytics results data that indicates a frequency with which the corresponding attack model successfully detected the particular attack." Appeal Br. 26 (Claims App. (emphasis added)). Claim 16 recites

substantially the same limitation in the computer-readable media of claim 15. *Id.* at 30. Appellant relies on substantially the same contentions it presented with respect to independent claim 8 to overcome the rejection to claims 2 and 16. *Id.* at 17–19, 20.

For the reasons given above with respect to the "resource usage measurements" limitation of independent claim 8, we are not persuaded that the Examiner erred in the obviousness rejection of claims 2 and 16, and we sustain that rejection. *See* Ans. 10–12.

e. Dependent Claim 3

In the devices of claim 1, claim 3 recites "the instructions, when executed by the hardware processor, cause the hardware processor to update the first set of attack models *in response to a triggering event*." Appeal Br. 26 (Claims App.) (emphasis added). Appellant relies on substantially the same contentions it presented with respect to independent claim 8 to overcome the rejection to claim 3. *Id.* at 21.

For the reasons given above with respect to the "triggering event" limitation of independent claim 8, we are not persuaded that the Examiner erred in the obviousness rejection of claim 3, and we sustain that rejection. *See* Ans. 12.

f. Dependent Claims 7, 12, and 20

In the devices of claim 1, claim 7 recites

> wherein the instructions further cause the hardware processor to:
>
> determine, based on the performance data that a particular attack model in the first set *performed worse than at least one other attack model included in the first set*; and
>
> in response to the determination, remove or change the

particular attack model.

Appeal Br. 27 (Claims App.) (emphasis added). Claims 12 and 20 depend from independent claims 8 and 15, respectively, and recite substantially the same limitation. *Id.* at 29, 31.

Di Pietro discloses

> SGE 402 or another device may evaluate the performance of the attack detector on these samples labeled by the expert. If the performance of the classifier is tolerable (e.g., satisfies a recall or precision value set by a user), this means that the classifier is already capable of correctly identifying the behavior as indicative of an attack. . . . *Otherwise, if the current version of the attack detector is unable to satisfy the required performance, SGE 402 may also update the attack detector by adding the traffic samples to the training data set for the relevant class and recomputing the attack detector.*

Di Pietro ¶ 68 (emphasis added). Thus, the Examiner finds

> [Di Pietro's] attack detector performance will be *worse* if it is unable to detect an unexpected behavior. As far as determin[ing] an attack model from another attack model, the prior art of Yen discloses the attack models can be put into different classes, and the templates can be used [or] refined during use as more knowledge is gathered about attack behavior.

Ans. 13 (emphasis added; citing Yen, 4:22–35).

Appellant contends that the Examiner fails to show either Di Pietro or Yen, alone or in combination, teaches or suggests comparing attack models to identify one that performed "worse" than another did. Appeal Br. 22–23. We agree. Neither the cited portion of Di Pietro nor that of Yen teaches or suggests comparing the performance of attack models, as opposed to identifying inadequate or different attack models. *See* Di Pietro ¶¶ 67–72: Yen, 4:25–35.

For the reasons given above, we are persuaded that the Examiner erred in the obviousness rejection of claims 7, 12, and 20, and we do not sustain that rejection.

g. Dependent Claim 13

In the methods of claim 8, claim 13 recites, "clustering attack models included in the first set to create at least two subsets of attack models, the clustering being based on at least one of performance or attack model characteristics of the attack models in the first set." Appeal Br. 29 (Claims App.). In the Final Action, the Examiner relies solely on Di Pietro to teach or suggest this limitation (Final Act. 15–16 (citing Di Pietro ¶¶ 43, 44)); however, in the Answer, the Examiner relies on Di Pietro and Yen to teach or suggest this limitation (Ans. 14 (citing Yen, 4:22–29; Di Pietro ¶¶ 56, 68)).

The Examiner finds

> Yen discloses clustering attack models in the first set to create at least two subsets of attack models, because Yen discloses different classes of attacks can be defined and the classes used to guide template creation/model. Yen discloses templates for such different classes of attack can be built and deployed for use.

Id. (citing Yen, 4:22–24). Thus, the Examiner concludes that "Yen disclose[s], '*clustering attack models included in the first set to create at least two subsets of attack models*.'" *Id.* We agree.

The Examiner further finds "Di Pietro discloses a GMM (Gaussian Mixture Model) or cluster-based model may be used for the expected traffic model (Di Pietro: para. 0056). The attack model, attack detector, can be evaluated based on performance of the attack detector (Di Pietro: para. 0068)." Ans. 14. Thus, the Examiner concludes, "Di Pietro discloses the

clustering being based on the performance of the attack models in the first set." *Id.* However, we understand that a Gaussian Mixture Model (GMM) or cluster-based model, as described in Di Pietro, is a method of analyzing data sets, and not a method for organizing models, such as attack models. *See,* http://leap.ee.iisc.ac.in/sriram/teaching/MLSP_16/refs/GMM_Tutorial_Reynolds.pdf. Consequently, we are not persuaded the Examiner shows that Di Pietro teaches or suggests "clustering being based on at least one of performance or attack model characteristics of the attack models in the first set," as recited in claim 13.

For the reasons given above, we are persuaded that the Examiner erred in the obviousness rejection of claim 13, and we do not sustain that rejection.

2. Obviousness Over Di Pietro, Yen, and Lin

The Examiner rejects claims 14 and 18 as obvious over the combined teachings of Di Pietro, Yen, and Lin. Final Act. 16–17. Claim 14 depends from independent claim 8 via intervening claim 13, and claim 20 depends directly from independent claim 15. Appeals Br. 29, 30. For the reasons given above, we sustain the rejection of claims 8 and 15, but not the rejection of claim 13. Because we do not sustain the Examiner's rejection of claim 13, we also do not sustain the Examiner's rejection of claim 14. Nevertheless, because Appellant does not contest the rejection of claims 14 and 18 separately (Appeal Br. 25), Appellant waives any arguments regarding the Examiner's findings concerning the teachings of Lin. For this reason, we sustain the rejection of claim 18.

NEW GROUND OF REJECTION OF CLAIM 1 UNDER 37 C.F.R. § 41.50(B)

In the Final Rejection, the Examiner rejected the pending claims as directed to a judicial exception to patent eligibility, without significantly more, and made findings supporting that rejection. *See* Final Act. 2–4, 7–9. Nevertheless, the Examiner withdrew the rejection in the Answer "due to new guidelines regarding 101." Ans. 3. "More specifically, [the Examiner found] independent claims 1, 8, and 15 have a practical application, because the attack model performance is used to determine whether to update the attack model by adding or [re]moving [an attack model to/from a first set of attack models]." *Id.* Although the Examiner withdrew Final Action's rejection under Section 101, we are not persuaded that the Examiner's finding of a practical application as a reason for withdrawing the rejection is consistent with the Office's guidance on Section 101, and, therefore, we consider here whether claim 1 is patent eligible under the Office's guidance. We cite to the Examiner's original findings where applicable.

We make the following new ground of rejection:

- Claim 1 is rejected under 35 U.S.C. § 101 as directed to an abstract idea without reciting additional elements amounting to significantly more than the abstract idea.

Patent Ineligible Claim

A. Section 101

An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. However, the U.S. Supreme Court has long interpreted 35 U.S.C. § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and

abstract ideas" are not patentable. *E.g.*, *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

In determining whether a claim falls within an excluded category, we are guided by the Court's two-part framework, described in *Mayo* and *Alice*. *Alice*, 573 U.S. at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 75–77 (2012)). In accordance with that framework, we first determine what concept the claim is "directed to." *See Alice*, 573 U.S. at 219 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.,* the use of a third party to mitigate settlement risk."); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk."). According to the Court, concepts determined to be abstract ideas and, thus, patent ineligible, include certain methods of organizing human activity, such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski*, 561 U.S. at 611); mathematical formulas (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 67 (1972)).

In *Diamond v. Diehr*, the claim at issue recited a mathematical formula, but the Court held that "a claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula." *Diamond v. Diehr*, 450 U.S. 175, 187 (1981). Having said that, the Court also indicated that a claim "seeking patent protection for that formula in the abstract . . . is not accorded the protection of our patent laws, and this principle cannot be circumvented by attempting to limit the use of the formula to a particular technological environment." *Id.* at 191 (citing *Benson* and *Flook*). Nevertheless, the Court noted that "[i]t

is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection." *Id.* at 187; *see also BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1352 (Fed. Cir. 2016) (Even if the individual components were known, "an inventive concept can be found in the ordered combination of claim limitations that transform the abstract idea of filtering content into a particular, *practical application* of that abstract idea" (emphasis added).).

If the claim is "directed to" an abstract idea, we next "must examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (quotation marks omitted). "A claim that recites an abstract idea must include 'additional features' to ensure 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].'" *Id.* (alterations in original) (quoting *Mayo*, 566 U.S. at 77). "[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Id.*

B. Office Patent Eligibility Guidance

In an effort to achieve clarity and consistency in how the Office applies the Court's two-part framework, the Office published revised guidance on the application of § 101. *See 2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (Jan. 7, 2019).[6] In Step One of

[6] "All USPTO personnel are, as a matter of internal agency management, expected to follow the guidance." *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. at 51; *see also October 2019 Update: Subject Matter Eligibility*, 1 (Oct. 17, 2019) ("Note, the feedback received

our analysis, we look to see whether the claims, as written, fall within one of the four statutory categories identified in § 101. *Id.* at 53 ("Examiners should determine whether a claim satisfies the criteria for subject matter eligibility by evaluating the claim in accordance with the criteria discussed in MPEP[7] § 2106, *i.e.*, whether the claim is to a statutory category (Step 1) and the *Alice/Mayo* test for judicial exceptions (Steps 2A and 2B)").

> Under the guidance, we then look to whether the claim recites:
>
> (1) Step 2A – Prong One: any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activity, such as a fundamental economic practice, or mental processes); and
>
> (2) Step 2A – Prong Two: additional elements that integrate the judicial exception into a practical application (*see* MPEP §§ 2106.05(a)–(c), (e)–(h)).

See 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. at 54–55 ("Revised Step 2A").

Only if a claim (1) recites a judicial exception *and* (2) does not integrate that exception into a practical application, do we then look to whether the claim:

> (3) adds a specific limitation beyond the judicial exception that is not "well-understood, routine, conventional" in the field (*see* MPEP § 2106.05(d)); or
>
> (4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

---

was primarily directed to examination procedures and, accordingly, this update focuses on clarifying practice for patent examiners. However, all USPTO personnel are expected to follow the guidance.").

[7] All Manual of Patent Examining Procedure ("MPEP") citations herein are to MPEP, Rev. 08.2017, January 2018.

See id. at 56 ("*Step 2B: If the Claim Is Directed to a Judicial Exception, Evaluate Whether the Claim Provides an Inventive Concept*.").

C. Step One – Claim 1 Is Directed to a Statutory Category

Appellant's independent claim 1 is directed to a device (i.e., a "machine"). Appeal Br. 26 (Claims App.). Thus, claim 1 is directed to a recognized statutory category.

D. Two-Part Alice/Mayo Analysis

1. Step 2A, Prong One – Claim 1 Recites an Abstract Idea

Applying the first part of the *Alice/Mayo* analysis (Step 2A), we determine that claim 1 recites "Mental processes—concepts performed in the human mind (including an observation, evaluation, judgment, opinion)." *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. at 52.

Although claim 1 recites *devices* comprising a hardware processor and a data storage device, the data storage device stores instructions that perform *processes* when executed by the processor. *See* Appeal Br. 26 (Claims App.). Claim 1 broadly recites (1) *identifying* a first set of attack models ("identify a first set of attack models, wherein a computing system is susceptible to a particular attack on the computing system and each attack model in the first set of attack models specifies a behavior of the particular attack on the computing system"); (2) *obtaining* performance data for each attack model that indicates a measure of attack performance data for a previous attack, from which it is determined the previous attack occurred ("obtain, for each attack model in the first set, performance data that indicates at least one measure of attack model performance for a previous use of the attack model in determining whether the particular attack occurred

on the computing system"); and (3) *updating* the first set of attack models based on the performance data to add or remove an attack model ("update the first set of attack models based on the performance data to add an attack model to the first set of attack models or remove an attack model from the first set of attack models"). *See id.* The Examiner finds "[t]he claims reciting the steps of 'identify', 'obtain', and 'update . . . are directed to an abstract idea as the claims describe an abstract idea of collecting and analyzing information.'" Final Act. 7.

The Office explains, "claims do recite a mental process when they contain limitations that can practically be performed in the human mind, including for example, observations, evaluations, judgments, and opinions." *October 2019 Update: Subject Matter Eligibility* at 7. For example, the Office notes "a claim to 'collecting information, analyzing it, and displaying certain results of the collection and analysis,' where the data analysis steps are recited at a high level of generality such that they could practically be performed in the human mind" recites a mental process. *Id.* (quoting *Elec. Power Grp., LLC v. Alstom, S.A.,* 830 F.3d 1350, 1356 (Fed. Cir. 2016)); *see* Final Act. 7 ("The concept described in said claims is similar to the concepts found by the courts to be abstract ideas of collecting and analyzing of *FairWarning IP, LLC v. Iatric Systems[, Inc.*, 839 F.3d 1089] (Fed. Cir. 2016 for details)."). Further, as the Office explains:

> Claims can recite a mental process even if they are claimed as being performed on a computer. . . . The courts have found claims requiring a generic computer or nominally reciting a generic computer may still recite a mental process even though the claim limitations are not performed entirely in the human mind.

October 2019 Update: Subject Matter Eligibility at 8.

Appellant contends claim 1 recites a "solution to improve computer technology and more specifically, set forth a way to manage computer attack models, which may be used to identify and handle security attacks on a computing system." Appeal Br. 8. In particular, Appellant contends:

> The claims set forth a solution to identify a set of attack models that are successful at detecting malware and are not overly resource intensive. Using claim 1 as an example, this claim recites that a computing system is susceptible to a particular attack on the computing system, and each attack model in a first set of attack models specifies a behavior of the particular attack on the computing system. The computing device of independent claim 1 recites that the hardware processor updates the first set of attack models based on performance data. As recited in claim 1, the "performance data . . . indicates at least one measure of attack model performance for a previous use of the attack model in determining whether the particular attack occurred in the computer system."

Id. at 9. We disagree.

In *SRI International Inc. v. Cisco Systems Inc.*, the Federal Circuit noted that:

> *Contrary to Cisco's assertion, the claims are not directed to just analyzing data from multiple sources to detect suspicious activity.* Instead, the claims are directed to an improvement in computer network technology. Indeed, representative claim 1 recites using network monitors to detect suspicious network activity based on analysis of network traffic data, generating reports of that suspicious activity, and integrating those reports using hierarchical monitors. The "focus of the claims is on the specific asserted improvement in computer capabilities"—that is, providing a network defense system that monitors network traffic in real-time to automatically detect large-scale attacks.

930 F.3d 1295, 1303 (Fed. Cir. 2019) (emphasis added; citations omitted); *see October 2019 Update: Subject Matter Eligibility* at 7 (citing *SRI Int'l*). Unlike the claims in *SRI International*, claim 1 merely recites a process for

identifying, gathering, and updating stored information about attacks. Therefore, we are persuaded that claim 1 recites a mental process.

2. Step 2A, Prong Two – The Abstract Idea Recited in Claim 1 Is Not Integrated Into a Practical Application.

The Examiner finds that claim 1 includes additional elements integrating the recited abstract idea into a practical application. Ans. 3. In particular, the Examiner finds that claim 1 has "a practical application, because the attack model performance is used to determine whether to update the attack model by adding or moving." *Id.*; *but see In re Comiskey*, 554 F.3d 967, 979 (Fed. Cir. 2009) ("In *Flook* the patentee argued that his claims did not seek to patent an abstract idea (an algorithm) because they were limited to a practical application of that idea—updating 'alarm limits' for catalytic chemical conversion of hydrocarbons. The Court rejected the notion that mere recitation of a practical application of an abstract idea makes it patentable, concluding that '[a] competent draftsman could attach some form of post-solution activity to almost any mathematical formula.'"); *Ex parte Gail et al.*, Appeal No. 2017-008600, 2019 WL 1776826, at *4 (PTAB Mar. 25, 2019) ("'Updating' can be met by incorporating new weather data either in the mind or by looking at new information and writing or remembering the updated forecast.") (Non-precedential). Integration into a practical application is evaluated by identifying whether there are additional elements, individually or in combination, that go beyond the judicial exception. *See 2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. at 54–55. However, the Examiner fails to show how this limitation amounts to a practical application consistent with the Office's guidance. We disagree with the Examiner's finding.

Claim 1 recites two components: a processor and a storage device coupled to the processor and storing instructions. Appeal Br. 26 (Claims App.). The Specification makes clear that these are generic components performing generic functions.[8] *E.g.,* Spec. ¶¶ 8 ("The behavior of attacks on computer systems, whether a single computer or a large network of many computing devices, can be modeled at a high level."), 14 ("Computing device 110 may be, for example, a personal computer, a server computer, mobile computing device, network device, or any other similar electronic device . . . ."), 15 ("Hardware processor 120 may be one or more central processing units (CPUs), semiconductor-based microprocessors, and/or other hardware devices suitable for retrieval and execution of instructions stored in machine-readable storage medium, 130."), 16 ("A machine-readable storage medium, such as 130, may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. Thus, machine-readable storage medium 130 may be, for example, Random Access Memory (RAM), non-volatile RAM (NVRAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage device, an optical disc, and the like."). Moreover, the steps recited in claim 1 describe generic functions of the processor and storage device. *Id.* ¶¶ 1 "Analytical devices and methods are also used to identify computer

[8] We acknowledge that some of the considerations at Step 2A, Prong Two, properly may be evaluated under the second part of the *Alice/Mayo* analysis (Step 2B of the Office guidance). *See* Final Act. 7–8. For purposes of maintaining consistent treatment within the Office, we evaluate those considerations under first part of the *Alice/Mayo* analysis (Step 2A of the Office guidance). *See* 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. at 55 nn.25, 27–32.

attacks at various stages, e.g., using symptoms or signatures of known attacks."), 14 (Computing device 110 is "capable of handling data, e.g., to manage computer attack models."), 15 ("Hardware processor 120 may fetch, decode, and execute instructions, such as 132-136, to control processes for computer attack model management."). The components, considered individually, do not link the abstract idea to a particular machine or technology or describe an improvement to the functioning of a computer. Final Act. 7. Viewed as an ordered combination, Applicant's claim simply recites the functions of data identification and collection and of updating the stored data, as performed by a generic computer utilizing generic computer components performing generic functions.[9] *See* Final Act. 7–8; *see* Spec. ¶¶ 13, 42, 49.

---

[9] It is well settled . . . that automating conventional activities using generic technology does not amount to an inventive concept. *See Alice*, 134 S.Ct. at 2358 (explaining that "if a patent's recitation of a computer amounts to a mere instruction to implement an abstract idea on ... a computer, that addition cannot impart patent eligibility") (internal alteration, citation, and quotations omitted); *Intellectual Ventures* [*I LLC v. Capital One Bank (USA)*], 792 F.3d [1363,] 1367 [(Fed. Cir. 2015)] ("claiming the *improved speed or efficiency* inherent with applying the abstract idea on a computer [does not] provide a sufficient inventive concept"); *Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Can.* (U.S.), 687 F.3d 1266, 1278 (Fed. Cir. 2012) ("[T]he fact that the required calculations could be performed *more efficiently* via a computer does not materially alter the patent eligibility of the claimed subject matter." (emphasis added)).

LendingTree, LLC v. Zillow, Inc., 656 F. App'x 991, 996 (Fed. Cir. 2016) (emphases added).

Thus, in view of Appellant's claim recitations and Specification, we are persuaded the rejected claim does not recite:

> (i) an improvement to the functioning of a computer;
>
> (ii) an improvement to another technology or technical field;
>
> (iii) an application of the abstract idea with, or by use of, a particular machine;
>
> (iv) a transformation or reduction of a particular article to a different state or thing; or
>
> (v) other meaningful limitations beyond generally linking the use of the abstract idea to a particular technological environment.

See MPEP § 2106.05(a)–(c), (e)–(h); *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. at 55. Thus, we conclude claim 1 does not integrate the judicial exception into a practical application, and claim 1 is directed to an abstract idea.

3. Step 2B – Claim 1 Does Not Recite Not Significantly More Than the Abstract Idea.

Because we find that claim 1 recites an abstract idea and does not integrate that abstract idea into a practical application, we now consider whether claim 1 includes additional limitations, such that the claim amounts to significantly more than the abstract idea. Applying the second part of the *Alice/Mayo* analysis, the Examiner concludes:

> The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the additional elements when considered both individually and as an ordered combination do not amount to significantly more than the abstract idea. It's noted that the claim recites some additional elements such as "hardware processor", and "data storage device". However, said additional elements, taken individually and as a combination, do not result in the claim amounting to significantly more than the abstract idea

> because "hardware processor", and "data storage device" are recited as performing generic computer content distributing functions routinely used in detecting fraud. Generic computer components recited as performing generic computer functions that are well understood, routine and conventional activities amount to no more than implementing the abstract idea with a computerized system. Therefore, the claim is directed to non-statutory subject matter.

Final Act. 7–8.

Appellant contends the Examiner fails to demonstrate that the additional components recited in the claims are well-understood, routine, and conventional, as required by in *Berkheimer v. HP Inc.,* 881 F.3d 1360 (Fed. Cir. 2018). Appeal Br. 11–12. Nevertheless, as noted above, the Specification shows the components are well-understood, routine, and conventional. Spec. ¶¶ 1, 8, 14–16; *see* Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision *(Berkheimer v. HP., Inc.)*, 3–4 (Apr. 19, 2018) (noting that the specification may evidence that components are well-understood, routine, and conventional); *see also In re TLI Commc'ns LLC Patent Litigation,* 823 F.3d 607, 614 (Fed. Cir. 2016) (citing to specification as showing a server that receives data, extracts classification information from the received data, and stores the digital images is insufficient to add an inventive concept). Consequently, we agree with the Examiner's assessment of these components.

As noted above, claim 1 recites the computer device performs the steps of *identifying* a first set of attack models, *obtaining* performance data for each attack model in the first set, and *updating* the first set of attack models based on the performance data to add or remove an attack model to the first set of attack models. The claim recites these computer functions at

a high level of generality. Further, the Specification does not describe that these recited steps are anything but generic computer functions, as are performed by any computer processing data. *E.g.*, Spec. ¶¶ 23 (identifying a first set of attack models), 24 (obtaining performance data), 25 (updating the first set of attack models based on the performance data), 47–50 (describing general methods of accomplishing the recited functions).

Our reviewing court has identified such functions as insufficient to show an inventive concept. In *Electric Power Group, LLC v. Alstom S.A.*, our reviewing court noted:

> The claims in this case do not even require a new source or type of information, or new techniques for analyzing it. As a result, they do not require an arguably inventive set of components or methods, such as measurement devices or techniques, that would generate new data. They do not invoke any assertedly inventive programming. Merely requiring the selection and manipulation of information—to provide a "humanly comprehensible" amount of information useful for users,—by itself does not transform the otherwise-abstract processes of information collection and analysis.

830 F.3d at 1355 (citations omitted); *see Content Extraction and Transmission LLC v. Wells Fargo Bank, Nat. Ass'n,* 776 F.3d 1343, 1348 (Fed. Cir. 2014) ("At most, CET's claims attempt to limit the abstract idea of *recognizing* and storing information from hard copy documents using a scanner and a computer to a particular technological environment."); *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716 (Fed. Cir. 2014) ("Adding routine additional steps such as *updating* an activity log, requiring a request from the consumer to view the ad, restrictions on public access, and use of the Internet does not transform an otherwise abstract idea [of showing an advertisement before delivering content] into patent-eligible

subject matter." (emphasis added)). Moreover, the ordering of these steps is entirely well-understood, conventional, and routine; performance data is gathered and used to update a previously identified set of attack models.

On this record, we determine that claim 1 recites generic computer components performing generic computer functions, which, considered individually or as an ordered combination, are well-understood, routine, and conventional; and claim 1 does not recite "significantly more" than the identified abstract idea. Final Act. 7–8. Therefore, we reject independent claim 1 under 35 U.S.C. § 101.

We have not reviewed independent claims 8 and 15 or the dependent claims. When prosecution resumes, the Examiner should consider the patent eligibility of at least claims 7, 12–14, and 20 in light of the Office's *2019 Revised Patent Subject Matter Eligibility Guidance* and this new ground of rejection of claim 1. We leave it to the Examiner to ascertain the appropriateness of any further rejections. Our decision not to enter a new ground of rejection for all or other pending claims should not be considered as any indication regarding the appropriateness of further rejection or allowance of the other pending claims. *See* MPEP § 1213.03.

DECISIONS

1. The Examiner did not err in rejecting claims 1–6, 8–11, and 15–19 as obvious over the combined teachings of Di Pietro and Yen, alone or in combination with Lin.
2. The Examiner erred in rejecting claims 7, 12–14, and 20 as obvious over the combined teachings of Di Pietro and Yen, alone or in combination with Lin.

3. We determine that claim 1 is unpatentable under 35 U.S.C. § 101, as directed to patent ineligible subject matter, without significantly more.
4. Thus, on this record, claims 1–6, 8–11, and 15–19 are not patentable; and claims 7, 12–14, and 20 are not unpatentable.

CONCLUSION

For the above reasons, we affirm the Examiner's decision rejecting claims 1–6, 8–11, and 15–19; reverse the Examiner's decision rejecting claims 7, 12–14, and 20; and enter a new ground rejecting claim 1.

In summary:

Claims Rejected	35 U.S.C. §	References	Affirmed	Reversed	New Ground
1–13, 15–17, 19, 20	103	Di Pietro, Yen	1–6, 8–11, 15–17, 19	7, 12, 13, 20	
14, 18	103	Di Pietro, Yen, Lin	18	14	
1	101	Eligibility			1
Overall Outcome			1–6, 8–11, 15–19,	7, 12–14, 20	1

This decision contains new grounds of rejection pursuant to 37 C.F.R. § 41.50(b). 37 C.F.R. § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 C.F.R. § 41.50(b) also provides that Appellant, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

> (1) *Reopen prosecution.* Submit an appropriate amendment of the claims so rejected or new Evidence relating to the claims so rejected, or both, and have the matter reconsidered by the

> examiner, in which event the prosecution will be remanded to the examiner. . . .
>
> (2) *Request rehearing.* Request that the proceeding be reheard under § 41.52 by the Board upon the same Record. . . .

Further guidance on responding to a new ground of rejection can be found in the Manual of Patent Examining Procedure § 1214.01. No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1).

AFFIRMED-IN-PART; 37 C.F.R. § 41.50(b)