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.
14/929,187	10/30/2015	Sudhakar Muddu	112509-8024.US01	3275

134200 7590 09/28/2020

Perkins Coie LLP - Splunk Inc.
P.O. Box 1247
Seattle, WA 98111-1247

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
09/28/2020	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):

patentofficecorrespondence@splunk.com
patentprocurement@perkinscoie.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SUDHAKAR MUDDU, CHRISTOS TRYFONAS, RAVI PRASAD BULUSU, and MARIOS ILIOFOTOU

Appeal 2019-002686
Application 14/929,187
Technology Center 2400

Before MAHSHID D. SAADAT, MARC S. HOFF, and IRVIN E. BRANCH, *Administrative Patent Judges*.

SAADAT, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

Pursuant to 35 U.S.C. § 134(a), Appellant[2] appeals from the Examiner's decision to reject claims 1–30, which constitute all the claims pending in this application. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

[1] An oral hearing scheduled for August 11, 2020, was waived.

[2] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42(a). Appellant identifies the real party in interest as Splunk Inc. Appeal Br. 2.

STATEMENT OF THE CASE

Appellant's disclosure is directed to "distributed data processing systems, and more particularly, to intelligence generation and activity discovery from events in a distributed data processing system." Spec. ¶ 3. Claim 1, which is illustrative of the invention, reads as follows:

> 1. A method comprising:
>
> receiving, by a computer system, event data representing a plurality of events on a computer network, the event data being indicative of a plurality of entities and at least one anomaly involved in the events;
>
> acquiring, for each event, an event-specific relationship graph indicative of entities involved in the event and one or more relationships between the entities involved in the event, each event-specific relationship graph including a plurality of nodes and a plurality of edges interconnecting the nodes, the nodes representing the entities involved in the event, each edge representing an interaction between a pair of entities involved in the event;
>
> acquiring anomaly data indicative of a plurality of security-related anomalies detected from the event data;
>
> combining the event-specific relationship graphs for the plurality of events with the anomaly data into a composite relationship graph, the composite relationship graph including nodes that represent the entities involved in the plurality of events and nodes that represent the anomalies detected based on the event data, wherein the entities involved in the plurality of events include at least two types of entities, the composite relationship graph further including edges that represent the relationships between the entities involved in the plurality of events and the anomalies; and
>
> detecting, by the computer system, a security threat by processing at least a portion of the composite relationship graph with a decision engine.

Claims 1–30 stand rejected under 35 U.S.C. § 102(a)(1) as being anticipated by Vasseur et al. (US 2016/0219066 Al; pub. July 28, 2016) ("Vasseur"). *See* Final Act. 3–14.

ANALYSIS

With respect to the rejection of claim 1, Appellant describes Vasseur's system as one that "utilizes graph-based anomaly detection at multiple devices in a computer network and a process of correlating the detected anomalies across the computer network." Appeal Br. 7 (citing Vasseur Abstract). According to Appellant, Vasseur's correlating process involves "one or more network events from [] one or more additional graph-based anomaly detection models." Appeal Br. 7–8. Based on this summary, Appellant contends that Vasseur does not disclose the recited step of "acquiring, for each event, an event-specific relationship graph indicative of entities involved in the event." Appeal Br. 8. Appellant refers to paragraphs 69–73 of Vasseur and argues the disclosed process relates to a graph-based model that shows different nodes or devices and the traffic between them, instead of the recited event-specific relationship graph that is specific to each event observed on the network. *See* Appeal Br. 8–10. Additionally, Appellant contends Vasseur's Figure 3B does not disclose the recited "combining the event-specific relationship graphs for the plurality of events with the anomaly data into a composite relationship graph" and instead, is directed to correlating events and identifying the nodes. *See* Appeal Br. 11–13.

In response, the Examiner explains

> Vasseur teaches acquiring, for each event, an event specific relationship graph (i.e., weighted/unweighted graphs according

> to volume of traffic [paragraph 0044 & Fig. 3A] and graph based model at certain time of the day [paragraph 0046 & Fig 3B] and indicative of entities involved in the event and one or more relationships between the entities involved in the event, each event-specific relationship graph including a plurality of nodes (i.e., Nodes represent actual devices, Fig 3A & 3B) and a plurality of edges interconnecting the nodes, the nodes representing the entities involved in the event, each edge representing an interaction between a pair of entities involved in the event (i.e., edges connecting the nodes representing traffic between the devices, Fig 3A & 3B).

Ans. 3–4. With respect to combining the event-specific relation graphs, the Examiner further explains Vasseur's Figure 3B shows a composite relationship graph that includes nodes and edges representing the entities involved in the anomaly. Ans. 4–5.

We are persuaded by Appellant's contentions that the Examiner erred. Although Vasseur's Figure 3B shows the nodes involved in two different events, anomaly #1 and anomaly #2, it represents two different graphs corresponding to different sets of devices. *See* Reply Br. 4. As also stated by Appellant, graphs 330 or 340 do not represent a composite relationship graph creates by combining two graphs containing anomaly data, but include the different deices distributed throughout the network. Reply Br. 4–5; Vasseur ¶ 46. We are further persuaded by Appellant's assertion that Vasseur's paragraph 46 describes Figure 3B as two graph-based models constructed by different devices in the network with overlapping nodes, which cannot be reasonably characterized as the recited composite relationship graph. Reply Br. 5–6. Appellant also asserts:

> Instead, every graph-based model described in Vasseur includes nodes that represent devices on a computer network. See e.g., graphs 300, 330, and 340 in FIGS. 3A-3B in Vasseur. At most,

> Vasseur describes detecting anomalies based on activity (represented as edges) between the devices (represented by the nodes). This is further supported by paragraph [0046] which describes, for example, "that an anomaly is detected from graph-based model 340 between nodes 326 and 332," and that "other anomalies may be detected between node pairs {320,326}, {320, 328}, and {326, 328}." Vasseur, par. [0046], emphasis added. Each of the nodes 320, 326, 328, and 332 represent devices and anomalies are detected based on traffic between the devices. None of these nodes represent the detected anomalies.

Reply Br. 6–7 (bold emphasis omitted). We agree. In other words, Vasseur uses the graph-based model including different devices or nodes and their corresponding traffic to detect anomalies based on their characteristics. Such representation does not consider or disclose a composite relationship graph for the involved nodes based on the event data, as recited in claim 1.

Summary

Accordingly, on the record before us, we do not sustain the 35 U.S.C. § 102(a)(1) rejection of claim 1, other independent claims 29 and 30, or claims 2–28 dependent therefrom.

CONCLUSION

In summary:

Claims Rejected	**35 U.S.C. §**	**Basis**	**Affirmed**	**Reversed**
1–30	102(a)(1)	Vasseur		1–30
Overall Outcome				1–30

REVERSED