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.
11/626,458	01/24/2007	Curtis M. Gearhart	RSW920060084US1 8152-0069	1255

73109 7590 02/27/2018

Cuenot, Forsythe & Kim, LLC
20283 State Road 7
Ste. 300
Boca Raton, FL 33498

EXAMINER
HERZOG, MADHURI R

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
02/27/2018	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):

ibmptomail@iplawpro.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte CURTIS M. GEARHART, CHRISTOPHER MEYER, LINWOOD H. OVERBY JR., and DAVID J. WIERBOWSKI

Appeal 2016-000847
Application 11/626,458
Technology Center 2400

Before MAHSHID D. SAADAT, JEAN R. HOMERE, and ALEX S. YAP, *Administrative Patent Judges*.

SAADAT, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants[1] appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 17–34.[2] We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

[1] According to Appellants, the real party in interest is IBM Corporation (App. Br. 1).

[2] Claims 1–11 have been cancelled (*id.*).

STATEMENT OF THE CASE

Appellants' invention relates to security services management for distributed security enforcement points using a set of security enforcement points for controlling communication flows (*see* Spec., ¶¶ [0001] and [0007]). Exemplary claim 17 under appeal reads as follows:

> 17. A security enforcement point separating a device within a first zone of protection from a device in a second zone of protection, comprising:
>
> an interface to a security server located in a third zone of protection; and
>
> at least one processor, wherein the at least one processor is configured to initiate and/or perform:
>
> controlling communication flows between the device in the first zone and the device in the second zone;
>
> performing a security service on the communication flows; and
>
> offloading, via the interface, a portion of the security service to security services logic within the security server, wherein
>
> the security enforcement point is disposed m one of the first and second zones of protection, and
>
> the third zone of protection is
>
> disposed separately from the first and second zones of protection, and
>
> a more trusted zone of protection than the first and second zones of protection.

REFERENCES and REJECTIONS

Claims 17–22 stand rejected under 35 U.S.C. § 101 as not being directed to patent eligible subject matter (*see* Final Act. 4–5).

Claims 17–19, 21–25, 27–31, 33, and 34 stand rejected under 35 U.S.C. § 102(b) as anticipated by Grantges (US 6,324,648 B1; Nov. 27, 2001), (*see* Final Act. 5–10).

Claims 20, 26, and 32 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Grantges (*see* Final Act. 11–12).

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellants' arguments that the Examiner erred. We are persuaded the Examiner erred in rejecting the claims under 35 U.S.C. § 101 for not being directed to patent eligible subject matter. We, however, are not persuaded the Examiner erred in rejecting the claims under 35 U.S.C. § 102(b) as anticipated by Grantges and under 35 U.S.C. § 103(a) as obvious over the cited reference, and we adopt as our own the findings and reasons set forth by the Examiner thereof. *See* Final Act. 4–12; Ans. 2–8. We highlight and address specific findings and arguments for emphasis as follows.

Section 101 Rejection

Independent claim 17 recites a security enforcement point comprising a processor for "controlling communication flows" and "performing a security service" as well as "offloading, . . ., a portion of the security service" and is, therefore, directed to one of the four statutory categories of patentability enumerated by 35 U.S.C. § 101 (process, machine, manufacture, or composition of matter). The Examiner finds claims 17–22 are "directed to an abstract idea because for example, the limitations of claim 17 merely recite a series of processes performed by an interface and a processor" but "do not include additional elements that are sufficient to

amount to significantly more than the judicial exception because the interface and processor are generic computer elements and do not add a meaningful limitation to the abstract idea because they would be routine in any computer implementation" (Final Act. 4–5). The Examiner refers to paragraph 33 of Appellants' Specification and finds the ordinary skilled artisan can construe this paragraph to imply that "the processor can be implemented in software" (Final Act. 5).

Appellants contend the Examiner erred in finding claim 17 is not directed to patent eligible subject matter (*see* App. Br. 5–7). Appellants argue that, contrary to the Examiner's assertion and consistent with DDR Holdings case that are tailored toward computer network technology, the claims are not directed to an "abstract idea" (App. Br. 6 (citing *DDR Holdings, LLC v. Hotels.Com, LP,* 773 F.3d 1245, 1257 (Fed. Cir. 2014)). With respect to their Specification and the reference to a processor in paragraphs 28–33, Appellants argue the recitation of "[a] data processing system suitable for storing and/or executing program code will include at least one processor coupled directly or indirectly to memory elements through a system bus" establishes the recited processor and the other elements refer to hardware or a machine (App. Br. 6–7).

We are persuaded by Appellants' arguments. The Supreme Court has set forth "a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts" (*Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2355 (2014) (citing *Mayo Collaborative Services v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1294 (2012))). According to this framework, a determination is made to consider whether the claims at issue are directed to

one of those concepts (i.e., laws of nature, natural phenomena, and abstract ideas) (*see id.*). If so, a further determination must be made to consider the elements of each claim both individually and "as an ordered combination" to determine whether the additional elements "transform the nature of the claim" into a patent-eligible application (*id.*).

First, we review claim 17 to determine whether it is directed to a patent ineligible concept, such as the "abstract idea" exception found by the Examiner. *See Mayo*, 132 S. Ct. at 1297; *see also* Final Act. 3. The claim recites steps of "controlling communication flows" as well as "performing a security service" and "offloading . . . , a portion of the security service." We find the recited steps are not directed to an abstract idea, but merely recite certain steps used to enforce network security.

Particularly, we are persuaded by Appellants' argument that the Examiner's generic, conclusory statement that the claim relates to a processing system suitable for storing and executing program code (*see* Ans. 4) does not address the actual the claim as a whole (Reply Br. 3–4). The recited limitations of claim 17, although generic, are not abstract and constitute functions that are widely known to be performed by a computer. In fact, similar to DDR holding, the appealed claims are "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks," and that the claimed invention did not simply use computers to serve a conventional business purpose (*see DDR Holdings, LLC v. Hotels.com*, 773 F.3d 1245, 1257 (Fed. Cir. 2014)).

Therefore, we are persuaded the Examiner erred in finding claims 17–22 recite patent-ineligible subject matter. Accordingly, we do not sustain the rejection of claims 17–22 under 35 U.S.C. § 101.

Section 102 Rejection

First, Appellants contend, recognizing firewall 32 as the first line of defense, Grantges does not teach proxy server 34 to be a security enforcement point (App. Br. 13 (citing Grantges Fig. 7)). More specifically, Appellants contend "the firewall 32 is between the private network side and the public network 26. Therefore, while the firewall 32 is illustrated as being connected to the proxy server 34, Grantges does not contemplate the proxy server 34 as being something different from the public network 26 regarding a different zone of protection" (*id.*).

These arguments are not persuasive because, as explained by the Examiner (Ans. 4–5), Grantges describes the proxy server as a security enforcement point by checking the validity of an authentication cookie because "DMZ proxy server 34 determines whether the incoming message contains a valid authentication cookie 90" and if the answer is "NO," sends a popup login screen to the user via secure connection 52 (*see* Grantges col. 14, ll. 29–55). The Examiner finds proxy server 34 in the DMZ server "is located between the insecure network 26 (e.g., the Internet) and the private network's first line of defense, for example, firewall system 32" (Ans. 5–6). We agree with these findings.

Second, Appellants contend:

> However, while these may be different zones, they are not different zones of protection. Grantges describes that in step 234, "web server 210 sends a redirect message to client computer 22." Thus, the proxy server 34 does not necessarily separate the web server 210 from the client computer 22. As a result, the proxy server 34 and web server 210, while possibly being in different zones, are within the same zone of protection - not separate zones of protection, as claimed.

(App. Br. 15). Lastly, Appellants contend Grantges describes a security service that "is being performed on the communication flows between the client 22 and the destination servers 28_1, 28_2" (App. Br. 16). Appellants assert the described communication flows are not "between the client 22 and the enterprise server 210" (*id.*).

The Examiner finds the cited portion of Grantges in column 14 discusses using proxy server 34 for controlling communication between the user computer on insecure network 26 (i.e., first zone) and the application web servers on the secure side of the firewall (i.e., second zone) (Ans. 6–7). We also agree with these findings.

Thus, Appellants' contentions do not persuade us of Examiner error in finding Grantges anticipates claim 17 because the references teaches all of the claim elements of independent claim 17. Accordingly, we sustain the Examiner's 35 U.S.C. § 102(b) rejection of claim 17, as well as claims 18, 19, 21–25, 27–31, 33, and 34 which are not argued separately (*see* App. Br. 12).

Section 103 Rejection

Appellants argue the patentability of claim 20 based on arguments similar to those presented with respect to the teachings of Grantges for claim 17 and add that the Examiner's conclusion of obviousness is "based upon a conclusory statement that is unsupported by an articulated reasoning with some rational underpinning" (App. Br. 18).

The Examiner provides a comprehensive response citing to the relevant passages in the applied reference and the proposed modifications. For example, the Examiner states:

> Grantges teaches the first zone to be an insecure internet zone and the second zone to be a demilitarized zone as claimed in claim 19 but does not teach wherein the first zone is a demilitarized zone, the second zone is an application zone. However, it is within the scope of one of ordinary skill in the art at the time of the invention to apply the principles of Grantges to zones specified in claim 20.

(Ans. 7). The Examiner relies on *KSR* holding and explains that the proposed modification would have been within "the ordinary capabilities of one skilled in the art" (Ans. 7–8 (citing *KSR Int'l Co., v. Teleflex Co.*, 550 U.S. 398 (2007))).

We agree with the Examiner and note that the Supreme Court has rejected the rigid requirement of demonstrating a teaching, suggestion, or motivation in the references to show obviousness. *See KSR*, 550 U.S. at 415–16; *see also In re Ethicon, Inc.*, 844 F.3d 1344, 1350 (Fed. Cir. 2017) ("*KSR* directs that an explicit teaching, suggestion, or motivation in the references is not necessary to support a conclusion of obviousness."). Instead, "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416. In the present case, the Examiner found that the ordinary skilled artisan would have found it obvious to apply the security enforcement scheme of Grantges to specific zones recited in claim 20 (Ans. 7–8). We find this articulated rationale to be sufficient to justify this modification which would merely require the ordinarily skilled artisan to combine prior art elements that perform their ordinary functions to predictably result in the claimed system.

Based on the Examiner's findings and analysis, which we adopt as our own, we sustain the Examiner's 35 U.S.C. § 103(a) rejection of claim 20, as well as claims 26 and 32 which are not argued separately (*see* App. Br. 16).

DECISION

We affirm the Examiner's decision to reject claims 17–34.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED