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.
13/620,255	09/14/2012	Shaun Wackerly	83037476	3854

56436 7590 11/02/2016
Hewlett Packard Enterprise
3404 E. Harmony Road
Mail Stop 79
Fort Collins, CO 80528

EXAMINER
ALATA, AYOUB

ART UNIT	PAPER NUMBER
2494	

NOTIFICATION DATE	DELIVERY MODE
11/02/2016	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):

hpe.ip.mail@hpe.com
mkraft@hpe.com
chris.mania@hpe.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SHAUN WACKERLY and JEREMY BROWN

Appeal 2015-006335
Application 13/620,255
Technology Center 2400

Before ERIC B. CHEN, HUNG H. BUI, and SHARON FENICK, *Administrative Patent Judges*.

CHEN, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1–19, all the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellants' invention relates to a network device that includes a security binding table and is configured to be coupled to a network and receive security information from a source device. (Abstract.)

Claim 1 is exemplary, with disputed limitations in italics:

> 1. A network device comprising:
>
> a security binding table having a plurality of entries each comprising a lookup portion and a match portion;
>
> the network device configured to couple to a network and receive security information, which includes a lookup portion and a match portion, from a source device coupled to the network; and
>
> a processor to:
>
> > compare the lookup portion of the received security information from the source device to the lookup portion of each entry of the security binding table and to compare the match portion of the received security information from the source device to the match portion of each entry of the security binding table to determine if there is a match; and
> >
> > *update the security binding table by adding an entry comprising the lookup portion and the match portion of the received security information from the source device based solely on when neither the lookup portion nor the match portion of the received security information from the source device matches any entry of the security binding table.*

Examiner's Rejections and References

(1) Claims 1–6 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

(2) Claims 1–3, 5, and 6 stand rejected under 35 U.S.C. § 102(b) as anticipated by Yadav (US 2009/0172156 A1; July 2, 2009).

(3) Claim 4 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Yadav and Szeto (US 2009/0260083 A1; Oct. 15, 2009).[1]

(4) Claims 7–10 and 12–19 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Yadav and Riley (US 2005/0163060 A1; July 28, 2005).

(5) Claim 11 stands rejected under 35 U.S.C. 103(a) as unpatentable over Yadav, Riley, and Cisco (Huynh Phi Long, CISCO EBOOK, ch. 6 (2007)).

ANALYSIS

§ 112, First Paragraph Rejection

We are persuaded by Appellants' arguments (App. Br. 7; *see also* Reply Br. 2) that the claim limitation "based solely on when neither the lookup portion nor the match portion of the received security information from the source device matches any entry of the security binding table" complies with the written description requirement under 35 U.S.C. § 112, first paragraph.

The Examiner found that there is "not . . . any support in the specification for an embodiment where it excludes any additional steps after deciding that 'neither the lookup portion nor the match portion of the received security information from the source device matches any entry of

[1] Appellants do not present any separate arguments with respect to the rejections of dependent claim 4 under 35 U.S.C. § 103(a). Thus, any such arguments are deemed to be waived.

the security binding table'" and "the specification does not describe any reason to exclude other additional steps in order to determine when to update the security binding." (Final Act. 6; *see also* Ans. 4–5.) We do not agree.

Appellants' Specification discloses the following:

> The white list is a security binding table that contains a list of entries identifying security information for approved hosts. A host device is then permitted (approved) only if its information is found as an entry in the white list of security table 47. If a host device is not found in the list, then it is implicitly considered to be disapproved.

(Spec. 5:20–25.) Appellants' Specification further discloses that "[i]n one example, sticky bindings are configured in security table 47 to be dynamically-learned only when neither the lookup portion nor the match portion of a host's security binding is found in white list 60." (Spec. 8:15–17.)

Because Appellants' Specification discloses that sticky bindings in security table 47 can "be dynamically-learned only *when neither the lookup portion nor the match portion of a host's security binding is found in white list 60*" (Spec. 8:15–17 (emphasis added)), such white list having "a list of entries identifying security information for approved hosts" (Spec. 5:21–22), Appellants' Specification provides written description support for the limitation "based solely on when neither the lookup portion nor the match portion of the received security information from the source device matches any entry of the security binding table."

Accordingly, we are persuaded by Appellants' arguments that "[o]ne cited section of the specification supporting this claim language, and which tracks the language of the claim quite closely, is found on page 8, lines 15–17 ['sticky bindings are configured in security table 47 to be dynamically

learned only when neither the lookup portion nor the match portion of a host's security binding is found in white list 60']." (Reply Br. 2.)

Thus, we do not agree with the Examiner that the Specification fails to provide written description support for the limitation "based solely on when neither the lookup portion nor the match portion of the received security information from the source device matches any entry of the security binding table."

Accordingly, we do not sustain the rejection of independent claim 1 under 35 U.S.C. § 112, first paragraph. Claims 2–6 depend from claim 1 and are rejected for the same reason. Therefore, we do not sustain the rejection of claims 2–6 under 35 U.S.C. § 112, first paragraph, for the same reasons discussed with respect to independent claim 1.

§ 102 Rejection—Yadav

We are unpersuaded by Appellants' arguments (App. Br. 9–12; *see also* Reply Br. 3) that Yadav does not describe the limitation "update the security binding table by adding an entry comprising the lookup portion and the match portion of the received security information from the source device based solely on when neither the lookup portion nor the match portion of the received security information from the source device matches any entry of the security binding table," as recited in independent claim 1.

The Examiner found that the core switch of Yadav, which determines if an Internet Protocol (IP) address and a Media Access Control (MAC) address are unique and updates the host information data table, corresponds to the limitation "update the security binding table by adding an entry comprising the lookup portion and the match portion of the received security

information from the source device based solely on when neither the lookup portion nor the match portion of the received security information from the source device matches any entry of the security binding table." (Final Act. 9; *see also* Ans. 6.) In particular, the Examiner found that "Yadav discloses the step of comparing the host information with a black list and/ or white list is optional [0023], and the device authentication may be incorporated into the method, which implies that the authentication step is also optional [0038]." (Ans. 6.) We agree with the Examiner.

Yadav relates to "providing multi-layer address security incorporating Layer 2 Media Access Control (MAC) addresses and corresponding Layer 3 Internet Protocol (IP) addresses for host machines on a routed access network." (¶ 2.) Figure 2 of Yadav illustrates a block diagram of a routed access network, including core switches, access switches, host machines, and end point machines. (¶ 17.) Yadav explains that "once the core switch 210 has received the host information data from the host device 241–245 and access switches 231–234, the data is then compared with the current host information data table 300 to check if the specific user or device is already currently connected 430," such check "to protect against spoofing, or stealing an IP address." (¶ 23.) Yadav further explains that "[s]hould it be determined that the IP address 302 and MAC address 301 are unique, the core switch 210 may then optionally compare the host information with a black list and/or a white list of host information." (*Id.*) Moreover, Yadav explains that "[s]hould the host device pass the authentication process, the core switch 210 would then update the host information data table 300" (¶ 24), however, "[i]n another aspect, the method may include device authentication, which may be performed by a server coupled to a switch in

the network" (¶38). Because Yadav explains that core switch 210 "optionally" compares IP address 302 and MAC address 301 with a black list and/or a white list and provides an alternative embodiment in which device authentication "may" be performed, Yadav discloses the limitation "update the security binding table by adding an entry comprising the lookup portion and the match portion of the received security information from the source device based solely on when neither the lookup portion nor the match portion of the received security information from the source device matches any entry of the security binding table."

Appellants argue that "[w]hile Appellants agree with the Examiner that the first additional step, that of comparing host information to a black list and/or a white list, is optional, Appellants vigorously disagree that use of the word 'may' at paragraph [0038] of Yadav means that the second additional step, that of authenticating the received host information, is optional." (App. Br. 11; *see also* Reply Br. 3.) Similarly, Appellants argue "[t]he drafter of the Yadav specification certainly cannot have intended for the word 'may' to mean not optional in paragraph [0034] and then subsequently intended the word 'may' to mean optional in paragraph [0038]." (App. Br. 12 (emphasis omitted).) However, by including the language "[i]n another aspect, the method *may include device authentication*," Yadav discloses at least two embodiments, including one embodiment in which device authentication is performed and an alternative embodiment in which device authentication is not performed (emphasis added).

Accordingly, we sustain the rejection of independent claim 1 under 35 U.S.C. § 102(b). Claims 2, 3, 5, and 6 depend from claim 1, and Appellants

have not presented any substantive arguments with respect to these claims. Therefore, we sustain the rejection of claims 2, 3, 5, and 6 under 35 U.S.C. § 102(b), for the same reasons discussed with respect to independent claim 1.

§ 103 Rejection—Yadav and Riley

We are unpersuaded by Appellants' arguments (App. Br. 14–15; *see also* Reply Br. 4) that the Examiner improperly combined Yadav and Riley.

The Examiner found that the policy server of Riley, which includes network polling, corresponds to the limitation "poll source devices." (Final Act. 15.) The Examiner concluded that "[i]t would have been obvious . . . to modify Yadav such that the invention further includes poll source devices" (*id.*) in order "to get current information about the source device" (Ans. 7). We agree with the Examiner.

Riley relates to communications and networking, in particular, "delivery of services over broadband infrastructures." (¶ 2.) Riley explains that "the policy server keeps track of the state of the network by maintaining state of all sessions that are currently active and by passively monitoring certain information that is being recorded at the various relevant network devices and components." (¶ 38.) Riley further explains that "[i]f the resource request fails because the CMTS [cable modem termination system] cannot locate the subscriber based on the IP address issued in the request by the policy server, the data collector uses this information to learn that the IP address to CMTS mapping has changed" and "[t]he data collector server re-polls the network to get updated information, and based on the new

information retries the request to the now current CMTS." (¶ 182.) Thus, Riley teaches the limitation "poll source devices."

A person of ordinary skill in the art would have recognized that incorporating the data collector server of Riley, which polls the network, with the network of Yadav, would improve Yadav by providing the advantage of monitoring such network. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) ("[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill."). Thus, we agree with the Examiner (Final Act. 15) that modifying Yadav to incorporate the policy server of Riley would have been obvious.

Appellants argue that

> regardless of the teachings of Riley, the person of ordinary skill in the art would not modify the teachings of Yadav so as to dynamically update an entry of a security binding table when a lookup portion of security information of a polled source device matches a lookup portion of an entry in the security binding table but the match portion of the security information of the polled device does not match the match portion of the entry in the security binding table, because such modification would defeat Yadev's stated purpose of blocking a network device from accessing the network under such conditions in order to protect the network against spoofing and unauthorized access.

(App. Br. 14 (emphasis omitted).) However, Appellants have not presented any evidence to support the arguments that "such modification would defeat Yadev's stated purpose of blocking a network device." Arguments of counsel cannot take the place of factually supported objective evidence. *See, e.g., In re Huang*, 100 F.3d 135, 139–40 (Fed. Cir. 1996).

Appellants also argue that "[t]he teachings of Riley are not at all related to security and access and assumes in its monitoring of how networks are being used that the users have already properly accessed the network" and "[t]his is not the case of Yadav, which is specifically focused on security information and the updating of entries in a security binding table based on such security information." (Reply Br. 4.) However, the Examiner relied upon Riley for the general teaching that network polling is well-known. (Final Act 15.) To the extent Appellants are arguing that Riley is not analogous art, we find that Riley's teachings regarding preventing disruption of a network by an end user (¶¶ 2, 4, 5) are reasonably pertinent to the particular problem with which the inventors were involved, namely preventing disallowed hosts from disrupting a network (Spec. 1:11–12). *See In re Clay*, 966 F.2d 656, 658–59 (Fed. Cir. 1992).

Therefore, the Examiner has properly combined Yadav and Riley to reject claim 7 under 35 U.S.C. § 103(a).

Accordingly, we sustain the rejection of claim 7 under 35 U.S.C. § 103(a). Claims 8–10 and 11 depend from claim 7, and Appellants have not presented any additional substantive arguments with respect to these claims. Therefore, we sustain the rejection of claims 8–10 and 11 under 35 U.S.C. § 103(a), for the same reasons discussed with respect to independent claim 7.

Independent claim 13 recites limitations similar to those discussed with respect to independent claim 7, and Appellants have not presented any additional substantive arguments with respect to these claims. We sustain the rejection of claim 7, as well as dependent claims 14–19, for the same reasons discussed with respect to claim 7.

§ 103 Rejection—Yadav, Riley, and Cisco

Although Appellants nominally argue the rejection of dependent claim 11 separately (App. Br. 16), the arguments presented do not point out with particularity or explain why the limitations of the dependent claims are separately patentable. Instead, Appellants merely argue "claim 11 depends from and further defines independent claim 7, which Appellants submit is in allowable form over the art of record." (*Id.*) We are not persuaded by these arguments for the reasons discussed with respect to claim 7, from which claim 11 depends. Accordingly, we sustain this rejection.

DECISION

The Examiner's decision rejecting claims 1–19 is affirmed.

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