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.
10/932,213	08/31/2004	Maarten E. Rits	000005-003900US	9891

68155 7590 02/01/2013
FOUNTAINHEAD LAW GROUP, PC
Chad R. Walsh
900 LAFAYETTE STREET
SUITE 301
SANTA CLARA, CA 95050

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
02/01/2013	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):

docketing@fountainheadlaw.com
vhernandez@fountainheadlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MAARTEN E. RITS, CEDRIC S.P. ULMER, CEDRIC R.J. HEBERT, LAURENT Y. GOMEZ, and PASCAL T.C. SPADONE

Appeal 2010-008442
Application 10/932,213[1]
Technology Center 2400

Before JEFFREY S. SMITH, STANLEY M. WEINBERG, and JOHN A. EVANS, *Administrative Patent Judges*.

EVANS, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) involving claims to dynamic computer security policy enforcement. The Examiner has rejected the claims as obvious and anticipated. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Rather than reiterate the arguments of Appellants and the Examiner, we refer to the Appeal Brief (filed Jan. 6, 2010), the Answer (mailed April 1,

---

[1] The real party in interest is SAP AG.

2010), and the Reply Brief (filed May 18, 2010). We have considered in this decision only those arguments Appellants actually raised in the Briefs. Any other arguments which Appellants could have made but chose not to make in the Briefs are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(iv).

STATEMENT OF THE CASE

The claims relate to methods for dynamic security enforcement including running an application with linked aspects and, upon determination that a security issue is present in the application, an aspect is written and linked to the application to address the security issue. (*See* Abstract).

Claims 1-22, 25-32, 34, and 36-41 are on appeal. Claims 1, 11, and 21 are independent. An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below:

> 1. A method for dynamic security enforcement comprising:
> running an application with linked aspects;
> detecting a security issue present in the application;
> determining a type of the security issue;
> generating an aspect to fix the security issue based on the type of the security issue; and
> linking the aspect to the application,
> wherein the application comprises a code statement for accessing the aspect, and wherein the aspect comprises code to fix a particular type of security issue, and wherein the particular type of security issue fixed is said determined type of security issue.

The claims are rejected as follows:

1. Claims 1-5, 7, 21, 22, 25-27, 29, 36, and 37 are rejected under 35 U.S.C. § 102(e) as anticipated by Dadhia (US 2005/0188419 A1, filed Aug. 13, 2004). (Ans. 3-11).

2. Claims 6 and 28 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Bangui (US 2006/0085645 A1, priority PCT/FR03/03877, Dec. 23, 2003). (Ans. 11-12).

3. Claims 8, 9, 30, and 31 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Johnson (US 7,131,001 B1, filed Oct. 11, 2000). (Ans. 12-13).

4. Claims 8, 10, 30, and 32 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and DeClouet (US 2004/0015718 A1, filed Jul. 22, 2002). (Ans. 13-14).

5. Claims 11-15 and 17 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Keim (US 2004/0205699 A1, filed Apr. 8, 2003). (Ans. 14-19).

6. Claim 16 is rejected under 35 U.S.C. § 103(a) as obvious over Dadhia, Keim, and Bangui. (Ans. 19-21).

7. Claims 18 and 19 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia, Keim, and Johnson. (Ans. 21).

8. Claims 18 and 20 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia, Keim, and DeClouet. (Ans. 22-23).

9. Claims 34 and 38 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Gelbard (US 2005/0027752 A1, priority Jul. 28, 2003. (Ans. 23-24).

10. Claims 39-41 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Coskun (US 5,764,958, issued Jun. 9, 1998). (Ans. 24-25).

Claim Groupings

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal on the basis of claims as set forth below. *See* 37 C.F.R. § 41.37(c)(1)(vii).

THE ANTICIPATION REJECTION

CONTENTIONS AND ANALYSIS

The Examiner has rejected claims 1-5, 7, 21, 22, 25-27, 29, 36, and 37 under 35 U.S.C. § 102(e) as anticipated by Dadhia. The Examiner finds that Dadhia discloses each claimed limitation. (Ans. 3-11).

Appellants argue claims 1-5 and 7, as a first group (App. Br 11) and argue claims 21, 22, 25-27, and 29, as a second group (App. Br 20). However, Appellants advance essentially the same contentions regarding the second group as for the first group. (App. Br. 20). We, therefore, consider claims 1-5, 7, 21, 22, 25-27, and 29 as a group. The issue advanced by Appellants relates to their allegations that the claims recite limitations not disclosed in the prior art.

Appellants contend that claim 1 recites a method of "dynamic security enforcement" and that the term "dynamic" is used to distinguish over the cited art because in contrast to other systems, "dynamic security enforcement" occurs when the application is running, not when an instance of the application is initiated. (App. Br. 11-12). The Examiner finds the recitation "dynamic" does not merit patentable weight because it occurs only in the preamble. (Ans. 26 (citing *In re Hirao*, 535 F.2d 67 (CCPA 1976); *Kropa v. Robie*, 187 F.2d 150, 152 (CCPA 1951))). Moreover, the Examiner finds that Dadhia discloses a dynamic protection system that identifies the

security level of an instance of an application that is to execute on a computer system. (Ans. 26). Appellants' Reply reiterates arguments advanced in the principle brief. (*See generally* Reply Br.).

We do not find Appellants' arguments to be persuasive. The Examiner has found that Dadhia discloses a "dynamic protection system [which] identifies the security level of an instance of an application that is to execute on a computer system." (Ans. 3 (emphasis omitted)). Appellants' argument that the Examiner failed to give patentable weight to the recitation "dynamic" because of its location in the preamble is not commensurate with the full scope of the rejection.

Appellants contend that claim 1 recites "running an application" which is distinct from an "instance of an application" and contend that Dadhia relates to an instance of an application. (App. Br. 12-13). The Examiner answers that "executing an application is equivalent to running an application." (Ans. 26). Appellants' Reply reiterates arguments advanced in the principle brief. (*See generally* Reply Br.).

Appellants' arguments are not persuasive because Appellants have not shown, factually, how it is possible to run an instance of an application without running the application.

Appellants contend that claim 1 recites "detecting a security issue" and "determining a type of the security issue." Appellants further contend that "security issue" refers to top-level security requirements, permissions, and initialization. (*See* App. Br. 14 (citing Spec. ¶¶ 0024, 0027; Fig. 4)). The Examiner finds that Dadhia discloses identifying whether an instance of application has been infected with a worm. The Examiner finds that a worm is a self-replicating program that will almost always cause at least some

harm to a network, even if only by consuming bandwidth. The Examiner concludes that the fact that a worm can cause damage to a network would make it a security issue. The Examiner further finds that Appellants' Specification has not defined "security issue" to preclude its ordinary and customary meaning. (Ans. 27).

We agree with the Examiner that, read broadly and consistently with the Specification, a "worm" would pose a "security issue" and that Appellants have not defined "security issue" so as to preclude a worm.

Appellants contend that claim 1 recites "detecting a security issue present in the application" which means that the application continues to function in its current state unless a security problem is detected. Appellants further contend that Dadhia discloses identifying security concerns only upon launch of an instance of an application. (App. Br. 16-17). We agree with the Examiner's finding, as discussed above, that a worm can cause damage to a network while application are running, thus making it a security issue. (Ans. 27).

Appellants contend that claim 1 recites an "application with linked aspects," thus, claim 1 is directed toward a specific type of application that includes "aspects" that are "linked." Appellants contend that these terms are defined at paragraph 0023 of the Specification. (App. Br. 27). The Examiner finds that "linked aspects" are merely key points in the application and that an instance of the application is a key point or component of the application. (Spec. ¶ 0015). We find Appellants' arguments not persuasive because Appellants illustrate, but do not define, "linked aspects" so as to preclude the Examiner's definition.

Appellants contend that the claim 1 recitations "generating an aspect . . . based on the type of the security issue," "linking the aspect to the application," and "running an application with linked aspects" are not taught by Dadhia. (App. Br. 19-20). We find this argument merely restates arguments previously discussed above and found not persuasive because Appellants have not acted as their own lexicographer to define their claim terms to the exclusion of the broader, but reasonable, interpretations found by the Examiner.

We now take Appellants' separate arguments in favor of claims 36 and 37.

Appellants contend that claim 36 recites "modifying byte-code during execution of the application." Appellants contend that Dadhia paragraph 0036, cited by the Examiner, relates to a file size in bytes and not to a "byte-code." (App. Br. 21). The Examiner finds that Dadhia discloses a rule may specify, *e.g.*, that it is satisfied by a certain type of message with a field indicating a file size greater than 1024 bytes, and the action of the rule may specify that the message should be discarded. (Ans. 10-11). The Examiner also finds that Dadhia discloses modifying byte-code:

> Dadhia discloses the protection system may collect the security level information of an instance of an application in various ways. Security level information may be stored in an instance-specific configuration file or a central registry in an instance-specific entry. The security level information may also be maintained by a patch installation component of an operating system. The protection system can access the configuration file or registry or send a request to the patch installation component to retrieve the security level information of the instance of the application. Alternatively, the protection system may subscribe to a service that publishes security level information as changes are made to the security level of an instance of an application.

(Ans. 29 (citing Dadhia ¶ 0015)). Appellants have not provided persuasive evidence or argument to rebut the Examiner's findings. Because Appellants do not address this finding, we are not persuaded that the Examiner has erred in this regard.

Appellants contend that Dadhia fails to disclose "at a plurality of method invocations," as recited in claim 37. Appellants contend that the Background (of the Specification) discusses embodiments that are directed toward aspect oriented programming, and that a feature of aspect oriented programming is "method invocations." Appellants contend that Dadhia (¶ 0016), cited by the Examiner, does not relate to aspect oriented programming (App. Br. 22). The Examiner disagrees with Appellants and has made specific findings relating to providing security patches to instances of a running application. (Ans. 29). Because Appellants have not specifically defined "method invocations" to exclude the Examiner's finding, we are not persuaded that Appellants have shown that the Examiner has erred.

THE OBVIOUSNESS REJECTIONS

CONTENTIONS AND ANALYSIS

Claims 6 and 28

Claims 6 and 28 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Bangui. (Ans. 11-12). Appellants do not dispute that Dadhia, as modified by Bangui, teaches each claimed limitation. Appellants contend that the Examiner has failed to properly articulate a reason to modify Dadhia with the teachings of Bangui. (App. Br. 23-26). We are not persuaded because Appellants fail to make out a fact-based case that the combination is improper. That is, Appellants have not factually responded to the Examiner

specific citations to the references nor to the reasons why the Examiner concludes it would have been obvious to combine the references. Arguments of counsel and discussions of caselaw, standing alone, cannot take the place of factually supported objective evidence. (*In re Huang*, 100 F.3d 135, 139-40 (Fed. Cir. 1996)). Attorney argument is not evidence. (*In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974)). Lawyer's arguments and conclusory statements, which are unsupported by factual evidence, are entitled to little probative value. (*In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997)).

Claims 8, 9, 30, and 31

Claims 8, 9, 30, and 31 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Johnson. (Ans. 12-13). Appellants contend that the Examiner has failed to establish that Dadhia is vulnerable to guessing a passcode through brute force and, therefore, has failed to establish that the addition of Johnson provides an advantage. (App. Br. 26-27). The Examiner finds that Dadhia discloses a security issue, but does not teach that the security issue is an initialization security issue. Nor does Dadhia teach that the initialization security issue is a key-length security issue. The Examiner finds that Johnson teaches employing encryption for data and verifying the length of a key and that Johnson teaches that the vulnerability of the system is a function of key length. (Ans. 12-13). We are not persuaded that the Examiner's reason for modifying Dadhia with Johnson is unreasonable.

Claims 8, 10, 30, and 32

Claims 8, 10, 30, and 32 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and DeClouet. (Ans. 13-14). Appellants do not dispute that Dadhia, as modified by DeClouet, teaches each claimed limitation. Appellants merely conclude that the Examiner has not provided a rational

basis for combining the references. (App. Br. 28-29). We are not persuaded that the Examiner has erred because, as discussed above, attorney argument is not evidence.

Claims 11-15 and 17

Claims 11-15 and 17 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Keim. (Ans. 14-19). Appellants do not dispute that Dadhia, as modified by Keim, teaches each claimed limitation. Appellants merely conclude that the Examiner has not provided a rational basis for combining the references. (App. Br. 30-31). We are not persuaded that the Examiner has erred because, as discussed above, attorney argument is not evidence.

Claim 16

Claim 16 is rejected under 35 U.S.C. § 103(a) as obvious over Dadhia, Keim, and Bangui. (Ans. 19-21). Appellants do not dispute that Dadhia, as modified by Keim and Bangui, teaches each claimed limitation. Appellants merely conclude that the Examiner has not provided a rational basis for combining the references. (App. Br. 31-32). We are not persuaded that the Examiner has erred because, as discussed above, attorney argument is not evidence.

Claims 18-20, 34, and 38-41

Claims 18 and 19 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia, Keim, and Johnson. (Ans. 21). Claims 18 and 20 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia, Keim, and DeClouet. (Ans. 22-23). Claims 34 and 38 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Gelbard. (Ans. 23-24). Claims 39-41 are rejected under 35 U.S.C. § 103(a) as obvious over Dadhia and Coskun. (Ans. 24-25).

Appellants do not dispute that Dadhia, as modified by any of Keim, Johnson, DeClouet, Gelbard, or Coskun, teaches each claimed limitation. Appellants merely conclude that the Examiner has not provided a rational basis for combining the references. (App. Br. 32-39). We are not persuaded that the Examiner has erred because, as discussed above, attorney argument is not evidence.

SUMMARY

We affirm the rejection of claims 1-22, 25-32, 34, and 36-41 as anticipated and/or obvious.

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

babc