

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ARNDT DOUGLAS EADE, HAZEL HEATHER FIX,
PAUL KETTLEY, and PETER SIDDALL

Appeal 2008-0805
Application 09/790,414
Technology Center 2400

Decided: November 28, 2008

Before LANCE LEONARD BARRY, HOWARD B. BLANKENSHIP, and
ST. JOHN COURTENAY III, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

A Patent Examiner rejected claims 1-24. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

A. INVENTION

The invention at issue on appeal controls access to resources in a data processing system. (Spec. 1.) According to the Appellants, access to resources is conventionally controlled via security settings or security definitions used to initialize a data processing system. Each computer program or user has access permissions which may be varied by a system administrator. The Appellants complain that issuing individual changes to access permissions on a resource-by-resource or user-by-user basis requires significant work. (*Id.* 36.)

In contrast, their invention groups security access control for a number of resources or users. Consequently, "a single security change request can be used to effect a change of access permissions associated with a number of separate or at least closely coupled resources." (*Id.*)

B. ILLUSTRATIVE CLAIM

Claim 1, which further illustrates the invention, follows.

1. A method of controlling access with at least first and second computer programs to system resources of a data processing system, the first and second computer programs having respective first security control definitions that govern access to the system resources, the method comprising the steps of:

providing a second set of security qualifiers comprising at least one second security qualifier applicable jointly to at least both of the first and second computer programs; and

providing a second security control definition corresponding to the at least one second qualifier, the second security control definition being arranged, in use, to influence

definition which are [sic] also applicable jointly to a plurality of computer/application programs.

(*Id.*) The Appellants make the following argument.

‘Default permissions’ as the Examiner contends are taught by Lewis (a phrase found only in Column 14 of the Lewis teaching) are different from the security qualifiers and security control definitions taught by this invention and the interaction among such elements found here is lacking in Lewis. This is the essence of the argument made here. See the discussions at Page 16, lines 16 et seq and Page 26 lines 11 et seq of the specification of the application on appeal

(Reply Br. 3-4, 12.) They also argue that "[t]he Examiner's position is that the claim language is disjunctive. It is not. The [claim] recitation is that both a second set of security qualifiers and a second set of definitions are provided and that they cooperate in a particular manner." (*Id.* 3, 11.)

A. ISSUE

Therefore, the issue is whether the Appellants have shown error in the Examiner's finding that Lewis discloses both a second security qualifier applicable jointly to first and second computer programs and a second security control definition corresponding to the second qualifier and used to influence jointly access by the first and second programs.

B. PRINCIPLES OF LAW

"[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)). "Moreover, limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d

1181, 1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)).

"[A]nticipation is a question of fact." *In re Hyatt*, 211 F.3d 1367, 1371-72 (Fed. Cir. 2000) (citing *Bischoff v. Wethered*, 76 U.S. (9 Wall.) 812, 814-15 (1869); *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997)). "A reference anticipates a claim if it discloses the claimed invention 'such that a skilled artisan could take its teachings in *combination with his own knowledge of the particular art and be in possession of the invention.*'" *In re Graves*, 69 F.3d 1147, 1152 (Fed. Cir. 1995) (quoting *In re LeGrice*, 301 F.2d 929, 936 (CCPA 1962)).

C. FINDINGS OF FACT

We agree with the Examiner's finding that "**there is no specific definition for the term 'security qualifiers' in the [S]pecification and the term is not specifically defined in the claims . . .**" (Answer 9.) Similarly, we find that neither the claims nor the rest of the Specification define the term "second security control definition."

D. ANALYSIS

We decline the Appellants' invitation to read into the claims "the discussions at Page 16, lines 16 et seq and Page 26 lines 11 et seq of the [S]pecification" (Reply Br. 5.) Furthermore, the Appellants' argument that "[t]he Examiner's position is that the claim language is disjunctive" (*id.* 3) fails to address the Examiner's individual findings that "[t]he second security qualifiers include the rights/permissions contained within default

permissions" (Answer 9) and that "[t]hese default permissions then yield a second security control definition" (*Id.*)

E. CONCLUSION

For the aforementioned reasons, the Appellants have shown no error in the Examiner's finding that Lewis discloses both a second security qualifier applicable jointly to first and second computer programs and a second security control definition corresponding to the second qualifier and used to influence jointly access by the first and second programs.

III. CLAIMS 3, 11, AND 19

The Examiner find that "Lewis et al. teach a mechanism is used in order to allow or deny access to a resource by application programs based on their associated group in col. 9, line 51 - col. 10, line 1: . . . ***The OAM*** [i.e., Object Authority Manager] ***maintains authorizations at the level of groups rather than individual users.***" (Ans. 10-11.) The Appellants argue that "[t]he OAM is something other than a security control definition as taught for the present subject invention, and is submitted as being non-equivalent." (Reply Br. 4.)

A. ISSUE

Therefore, the issue is whether the Appellants have shown error in the Examiner's finding that Lewis discloses the second security control definition.

B. PRINCIPLE OF LAW

"Argument in the brief does not take the place of evidence in the record." *In re Schulze*, 346 F.2d 600, 602 (CCPA 1965) (citing *In re Cole*, 326 F.2d 769, 773 (CCPA 1964)).

C. FINDINGS OF FACT

The Appellants' argument is based on the premise that the Examiner is reading the claimed security control definition on Lewis' OAM.

D. ANALYSIS

This is not the case. To the contrary, the Examiner seems to read the claimed definition on Lewis' "rights/permissions" (Answer 9), which may be managed by the OAM. *See Lewis*, col. 9, ll. 51-62. Furthermore, the Appellants do not explain how, let alone show evidence to substantiate their argument that, "[t]he OAM is something other than a security control definition" (Reply Br. 4.)

E. CONCLUSION

For the aforementioned reasons, the Appellants have shown no error in the Examiner's finding that Lewis discloses the second security control definition.

IV. CLAIMS 4, 12, AND 20

The Examiner makes the following findings.

Lewis et al. teach that system access can be changed by invoking the first and second definitions in a particular sequence, since in one example, the default permissions may be

changed and after that occurs, various other permissions that the subject contains for that particular resource may also be added or deleted and thereby modified. Let us consider the example given in Lewis et al. in col. 14, lines 52-67: "The commands required to establish these permissions for the groups concerned are:

```
chgrp SNAadmin/var/SNAauthorisation/SNAlink/  
HOST1/attributes;
```

```
chgrp SNAuser /var/SNA/authorisation/SNAlink/  
HOST1/data;
```

```
chmod 760/var/SNA/authorisation/SNAlink/  
HOST1/attributes
```

```
chmod 770/var/SNA/authorisation/SNAlink/  
HOST1/data
```

This example uses an authorisation file structure which keeps the files with the resources, and which sets authorisations [sic] according to whether a subject is the resource owner, a member of the same subject group as the owner, or outside of the group." Given this example, there are two subjects in a group, one of which is also the owner of the resource. The two subjects have a second security control definition which includes the default permissions given for that group which may be modified. Additionally, one of the subjects also has a first security control definition showing that it is the owner and thus having additional permissions, which can also be modified if that subject at one point gave up it's ownership to the resource. Thus, this example shows that Lewis et al teach changing permissions to the first and second security control definitions in a particular sequence.

(Ans. 14-15.) The Appellants argue that some of "[t]his is unwarranted wild speculation **about applicant's invention.**" (Reply Br. 6 (emphasis added).)

A. ISSUE

Therefore, the issue is whether the Appellants have shown error in the Examiner's findings about Lewis.

B. FINDINGS OF FACT

The Appellants' argument is based on the premise that the Examiner's findings are "about applicant's invention." (Reply Br. 6.)

C. ANALYSIS

This is not the case. To the contrary, the Examiner's findings are about Lewis.

D. CONCLUSION

For the aforementioned reasons, the Appellants have shown no error in the Examiner's findings about Lewis.

V. CLAIMS 5, 6, 13, 14, 21, AND 22

Regarding claims 5, 13, and 21 the Examiner finds that "Lewis et al. teach that each subject has different rights depending on their level of access and the resource at hand, i.e. the first security control definitions that govern access to the system resources in col. 4, line 67 - col. 5, line 14" (Ans. 15.) Regarding claims 6, 14, and 22 he further finds that "Lewis et al. teach that subjects in a group are given default permissions, where these permissions enable or disable the type of access that subject will have to a resource (where there are many resources in a system) in col. 5, lines 42-65" (*Id.* 17.) The Appellants argue that "[a]n operating system permission

simply functions at a different level and differently from the security definitions here taught." (Reply Br. 7, 8.)

A. ISSUE

Therefore, the issue is whether the Appellants have shown error in the Examiner's finding that Lewis discloses that an associated security operation is either enabled or disabled in relation to a first or a second identifiable system resource.

B. FINDINGS OF FACT

The Appellants do not specify, let alone shown evidence of, the level at which the claimed security definitions allegedly function. Nor have they explained how, let alone shown evidence to substantiate their argument that, the Lewis' permissions function differently than the claimed security definitions.

C. CONCLUSION

For the aforementioned reasons, the Appellants have shown no error in the Examiner's finding that Lewis discloses that an associated security operation is either enabled or disabled in relation to a first or a second identifiable system resource.

VI. CLAIMS 7, 15, AND 23

The Examiner finds that "Lewis et al. teach that subjects in a group are given default permissions, where these permissions enable or disable the type of access that subject will have to a resource (where there are many

resources in a system) in col. 5, lines 42-65" (Ans. 18.) The Appellants argue that their "attorney can find in that passage no discussion of accessibility, common or controlled." (Reply Br. 10.)

A. ISSUE

Therefore, the issue is whether the Appellants have shown error in the Examiner's finding that Lewis discloses common accessibility of a resource.

B. PRINCIPLES OF LAW

Anticipation "is not an 'ipsissimis verbis' test." *In re Bond*, 910 F.2d 831, 832-33 (Fed. Cir. 1990) (citing *Akzo N.V. v. United States Int'l Trade Comm'n*, 808 F.2d 1471, 1479 n.11 (Fed. Cir. 1986)). "An anticipatory reference . . . need not duplicate word for word what is in the claims." *Standard Havens Prods. Inc., v. Gencor Indus. Inc.*, 953 F.2d 1360, 1369 (Fed. Cir. 1991).

C. FINDINGS OF FACT

The passage of Lewis cited by the Examiner includes the following disclosure: "It is also preferred to automatically assign default authorisations [sic] to users when they create a resource. The default settings for subjects' authorisations [sic] may be definitions stored in administration files of the authorisations [sic] for named subject groups." (Col. 5, ll. 41-45.)

D. ANALYSIS

Although the passage does not use the word "accessibility," we agree with the Examiner's finding that setting authorizations to access a resource implies that the resource is accessible. We also agree that a group authorization implies that the resource is commonly accessible by member of the group.

E. CONCLUSION

For the aforementioned reasons, the Appellants have shown no error in the Examiner's finding that Lewis discloses common accessibility of a resource.

VII. CLAIMS 2, 10, AND 18

The Examiner makes the following admission.

Not explicitly disclosed by Lewis et al. is the method, system, or computer program product in which first and second security definitions represent a security hierarchy in which the second security control definition prevails over the first security control definition such that access to system resources is controlled by the second security control definition in the absence of invoking the first security control definitions.

(Ans. 5-6.) He finds that "Lewis et al. specifically mention using hierarchical levels of access for performing various operations in col. 3, lines 44-50" (*id.* 49) and that "using the information mentioned by Lewis et al. in the background of the invention in combination with the summary and detailed description disclosed by Lewis et al., the combination yields the limitation presented in claim 2" (*id.*). The Appellants argue that "there is no suggestion in Lewis of the sequence of actions in a definition array as recited in Claim 2." (Reply Br. 18.)

A. ISSUE

Therefore, the issue is whether Examiner has shown that Lewis would have suggested a security hierarchy in which the second security control definition prevails over the first security control definition such that access to system resources is controlled by the second security control definition in the absence of invoking the first security control definition.

B. PRINCIPLES OF LAW

"In rejecting claims under 35 U.S.C. § 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532 (Fed. Cir. 1993) (citing *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992)). Furthermore, "[t]he Patent and Trademark Office (PTO) must consider all claim limitations when determining patentability of an invention over the prior art." *In re Lowry*, 32 F.3d 1579, 1582 (Fed. Cir. 1994) (citing *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983)).

C. FINDINGS OF FACT

The part of Lewis cited by the Examiner does mention "a hierarchy of levels of authorization" (Col. 3, l. 55.)

D. ANALYSIS

The hierarchy does not specify, however, that a second security control definition prevails over a first security control definition such that access to system resources is controlled by the second security control

definition in the absence of invoking the first security control definition. To the contrary, it merely means that "if one entity is authorised [sic] to perform an operation then all entities having a higher authorization level are also authorised [sic] and so need not be listed in the" (*id.* ll. 56-58) in an access control list.

E. CONCLUSION

For the aforementioned reasons, the Examiner has not shown that Lewis would have suggested a security hierarchy in which the second security control definition prevails over the first security control definition such that access to system resources is controlled by the second security control definition in the absence of invoking the first security control definition.

VIII. ORDER

We affirm the rejection of claims 1, 3-9, 11-17, and 19-24 but reverse the rejection of claims 2, 10, and 18.

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

AFFIRMED-IN-PART

rwk

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709