

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte YEHIA S. BEYH

Appeal 2008-0721
Application 10/207,654
Technology Center 2100

Decided: August 12, 2008

Before ALLEN R. MACDONALD, JAY P. LUCAS, and
ST. JOHN COURTENAY III, *Administrative Patent Judges*.

COURTENAY, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-9, 11-19, 21-30, and 32. Claims 10, 20, and 31 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

THE INVENTION

The disclosed invention relates generally to improved methods and systems for integrating a security protocol into an existing network environment. More particularly, Appellant's invention is directed to a method of establishing secure communication between a client and server computer on a network, the method comprising the steps of intercepting certain calls issued by the client, and substituting a security library for a working library of the client, the security library enabling operation of the issued call using a predefined security protocol (Spec. 2).

Independent claim 1 is illustrative:

1. In a computer network having a client computer and a server computer, a computer-implemented method of establishing a secure connection between the client and the server, comprising:
 - (A) intercepting a particular call issued by the client to the server;
 - (B) determining whether the particular call is to be executed using the secure connection;
 - (C) if it is determined that the particular call is to be executed using the secure connection, then:
 - (C) (1) substituting a security library for a working library of the client, the security library enabling execution of the particular call using a predefined security protocol; and
 - (C) (2) establishing the secure connection between the client and the server using the security library.

Appeal 2008-0721
Application 10/207,654

THE REFERENCES

The Examiner relies upon the following reference as evidence in support of the anticipation rejection:

SSH Sentinel, White Paper, Version 1.0, 1-35 (2001).

The Examiner relies upon the following two references as extrinsic evidence in support of the anticipation rejection:

SSH IPSEC Express Toolkit Integration with Customer Applications, White Paper, Version 4.1, total pages 21 (2001).

SSH Secure Shell, White Paper, Version 1.0, total pages 19 (2001).

THE REJECTION

Claims 1-9, 11-19, 21-30, and 32 stand rejected under 35 U.S.C. § 102(a) as being anticipated by SSH Sentinel.

PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 102, “[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation.” *Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375-76 (Fed. Cir. 2005) (citation omitted).

Extrinsic evidence may be used to explain but not expand the meaning of terms and phrases used in the reference relied upon as anticipatory of the claimed subject matter. *In re Baxter Travenol Labs.*, 952 F.2d 388, 390 (Fed. Cir. 1991). See also MPEP § 2131.01(II.).

FINDINGS OF FACT

The following Findings of Facts (FF) are shown by a preponderance of the evidence.

1. SSH is an abbreviation for Secure Shell protocol (Spec. 7, ll. 22-23).
2. The SSH Secure Shell reference (considered as extrinsic evidence to explain the meaning of the term(s) used in the SSH Sentinel reference) discloses that the Secure Shell protocol secures connections over the Internet by encrypting passwords and other data. Once launched, the Secure Shell protocol transparently provides strong authentication and secure communications over insecure networks (*see* SSH Secure Shell, p. 5, ¶1).
3. The SSH Sentinel reference also implements the IPSec protocol using an “IPSec engine [that] is responsible for performing the appropriate security transformations on the data packets.” (SSH Sentinel, p. 23, ¶1).
4. The SSH Sentinel reference discloses intercepting data packets (p. 23, Fig. 8; *see also* p. 24, ¶1).
5. Calls between a client and a server are made using protocols (such as IPSec, IP, etc.), where data is transferred using packets (*see* SSH Sentinel, p. 24, i.e., “SSH IPSec packet interceptors . . .”; p. 27, l. 1, i.e., “IP packet filtering . . . ”).
6. SSH Sentinel discloses that “IPSec automatically secures all traffic between the two hosts” (p. 27, ¶4).

7. The SSH Sentinel disclosure of the word “if” followed by a condition (i.e., “if the engine has the filter code for the packet available”), is a step of determination (SSH Sentinel, p. 24, ¶1).
8. SSH Sentinel discloses that the SSH Sentinel filter code, generated by the policy manager, is a script that performs the required security transformations on each packet (p. 24, ¶1).

ANALYSIS

We consider the Examiner’s rejection of claims 1-9, 11-19, 21-30, and 32 as being anticipated by the SSH Sentinel reference. Since Appellant’s arguments with respect to this rejection have treated these claims as a single group which stand or fall together, we select independent claim 1 as the representative claim for this rejection because we find it is the broadest claim before us. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Extrinsic Evidence used in support of Anticipation

We begin our analysis by noting that the Examiner relies upon two external references as extrinsic evidence to explain the meaning of the term(s) used in the SSH Sentinel reference.¹

Here, we note that Appellant does not contest the Examiner’s reliance upon the aforementioned extrinsic evidence for definitional support.

¹ The Examiner relies upon “SSH IPSEC Express Toolkit Integration with Customer Applications” and "SSH Secure Shell" as extrinsic evidence to explain the meaning of term(s) used in the primary "SSH Sentinel" reference (Ans. 3).

Therefore, we consider the extrinsic evidence only to the extent that it is used to explain but not expand the meaning of terms and phrases used in the SSH Sentinel reference.

For example, the SSH Sentinel reference makes reference to the “SSH IPSEC Express Toolkit” on page 13 (¶2). Therefore, we limit our consideration of the extrinsic “SSH IPSEC Express Toolkit Integration with Customer Applications” reference to merely providing an explanation of the meaning of the term “SSH IPSEC Express Toolkit.” In particular, the extrinsic “SSH IPSEC Express Toolkit Integration with Customer Applications” reference offers a broad explanation of the term “SSH IPSEC Express Toolkit,” as follows:

The SSH IPSEC Express Toolkit is a full, portable implementation of the IPSec protocol. The toolkit can be used by vendors of routers, access routers, VPN devices and firewalls. It is also suitable for all other users who need to add standards-based security features into their existing or new products. It provides highly efficient and unrestricted cryptography for maximum security and efficiency. (“SSH IPSEC Express Toolkit Integration with Customer Applications,” p. 2, ¶1).

In addition, we consider both external references to the extent that they providing an explanation of the meaning of the term SSH protocol (“Secure Shell Protocol”) (FF 1). In particular, the extrinsic "SSH Secure Shell" reference offers a broad explanation of the term “Secure Shell,” as follows:

Secure Shell secures connections over the Internet by encrypting passwords and other data. Once launched, it

transparently provides strong authentication and secure communications over insecure networks.
("SSH Secure Shell," p. 5, ¶1) (FF 2).

Arguments

In traversing the anticipation rejection, Appellant contends that several specific limitations of claim 1 are not disclosed by the SSH Sentinel reference (Br. 12-15). For convenience, we reference these limitations as A, B, C, and C2 *infra* (using the same nomenclature used in claim 1):

- (A) intercepting a particular call issued by the client to the server;
- (B) determining whether the particular call is to be executed using the secure connection;
- (C) if it is determined that the particular call is to be executed using the secure connection . . .
- (C) (2) establishing the secure connection . . .

Regarding limitation A, Appellant contends that the SSH Sentinel first establishes a secure connection in response to the user entering the address to which a secure connection is to be established, and once the secure connection is established, SSH Sentinel automatically secures all traffic between the two hosts. Appellant points to page 27 of the SSH Sentinel reference for support (Br. 13).

Thus, Appellant contends that instead of disclosing establishing secure connections between the client and server on a call-by-call basis, SSH Sentinel discloses manually establishing a secure connection between the

client and server, and then using that secure connection for *all* subsequent calls between the client and server (Br. 14).

During prosecution, “the 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)). Here, the Examiner is reading the claimed step of intercepting on Fig. 8 of the SSH Sentinel reference which discloses that packets are intercepted using the SSH IPSEC Packet Interceptor (Ans. 8; *see also* SSH Sentinel, p. 24, ¶1).

After considering the claim as a whole, we conclude that the broad language of Appellant’s claim 1 does not preclude the interpretation proffered by the Examiner. In particular, we agree with the Examiner’s reasoning that intercepting *all* calls (as disclosed by SSH Sentinel, p. 27, ¶4) also intercepts *particular* calls (Ans. 7) For example, if calls A-Z are intercepted, then *each* of calls A-Z is intercepted, e.g., “particular call” A is intercepted, “particular call” B is intercepted . . . and, “particular call” Z is intercepted in seriatim. *See* SSH Sentinel, p. 27, ¶4.

Further with respect to limitation A, Appellant contends that SSH Sentinel could not establish the secure connection between client and server after intercepting a particular call issued by the client to the server, because in the case of SSH Sentinel, the secure connection has already been established *before* the client begins issuing calls to the server (Br. 15).

We note that SSH Sentinel discloses the interception of data packets, followed by security transformations on each packet, as follows:

A data packet is trapped by the SSH IPsec packet interceptors and forwarded to the IPsec engine. If the engine has the filter code for the packet available, it simply runs the code on the

packet. The filter code, generated by the policy manager, is simply a script that performs the required security transformations on the packet.
(SSH Sentinel, p. 24, ¶1).

Thus, SSH Sentinel discloses intercepting packets (i.e., data associated with a call corresponding to limitation (A)), and then performing the required security transformations on each packet, but only *if* the engine has the filter code for the packet available, where the filter code is a script that performs the required security transformations on the packet (*id.*) (*see also* FF 3, FF 4, FF 6).

Regarding the claimed (B) limitation of “determining,” we note that SSH Sentinel expressly discloses testing for a condition: i.e., “[i]f the engine has the filter code for the packet available, it simply runs the code on the packet.” (*id.*). Thus, we find that the SSH Sentinel disclosure of the word “if” followed by a condition (i.e., “if the engine has the filter code for the packet available”), is a step of determination (FF 7). SSH Sentinel further discloses that the SSH Sentinel filter code, generated by the policy manager, is a script that performs the required security transformations on each packet (*id.*) (FF 8). Therefore, we find that SSH Sentinel discloses determining whether the call (i.e., particular call) is to be executed using the secure connection *after* a step of intercepting, as claimed.

While we agree with Appellant that SSH Sentinel discloses the use of a security policy that applies to *all* traffic, we nevertheless note that SSH Sentinel expressly discloses that “IPSec *automatically* secures all traffic between the two hosts” (p. 27, ¶4, emphasis added). Therefore, we find that the “IPSec” protocol software performs the “automatic” securing of all

traffic in accordance with the sequential packet interception and determination steps discussed *supra* (*see also* SSH Sentinel, p. 24, ¶1).

Appellant also argues portions of limitations (C) and (C2), as follows:

The SSH Sentinel White Paper, in contrast, does not disclose . . . establishing the secure connection if it is determined that the *particular call* is to be executed using the secure connection. (Br. 12, ¶2).

As claimed, the corresponding limitations are recited as follows:

(C) if it is determined that the particular call is to be executed using the secure connection . . .

(C) (2) establishing the secure connection . . .

(Claim 1).

To the contrary, we find that SSH Sentinel discloses establishing a secure connection if it is determined that a particular call is to be executed using the secure connection, as per our discussion of the sequential packet interception and determination steps discussed *supra* (*see* SSH Sentinel, p. 24, ¶1; *see also*, FF 7).

For at least the aforementioned reasons, we find that the weight of the evidence supports the Examiner's position. Because we conclude that Appellant has not shown the Examiner erred, we sustain the Examiner's rejection of independent claim 1 (and claims 2-9, 11-19, 21-30, and 32 that fall therewith), as being anticipated by SSH Sentinel. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Appeal 2008-0721
Application 10/207,654

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that Appellant has not met his burden of showing that the Examiner erred in rejecting claims 1-9, 11-19, 21-30, and 32 under 35 U.S.C. § 102(a) for anticipation. Therefore, these claims are not patentable.

DECISION

We affirm the Examiner's decision rejecting claims 1-9, 11-19, 21-30, and 32.

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

rwk

IP Administration, Legal Dept. M/S 35
Hewlett-Packard Com.
P.O. Box 272400
Fort Collins CO 80527-2400