

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte THOMAS JAY BILLHARTZ

Appeal 2008-2526
Application 10/197,148¹
Technology Center 2400

Decided: January 15, 2009

Before JAMES D. THOMAS, KENNETH W. HAIRSTON, and
JEAN R. HOMERE, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1 through 4, 6 through 24, 26, 27, 29 through 34, and 36 through 42. Claims 5, 25, 28, and 35 have been canceled. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

¹ Filed on July 17, 2002. The real party in interest is Harris Corp.

The Invention

Appellant invented a mobile ad-hoc network (MANET) for authenticating mobile nodes thereon sharing a common radio channel. (Spec. 1.) As shown in Figure 1, the MANET includes a first node having a first public key and a first private key; a second node (12) having a second public key and a second private key; and a certifying authority (14) having a public authentication key, and a private authentication key. Upon generating an authentication request, the first node (11) receives from the certifying authority (14) a certificate of authenticity along with a second public key. The first node then decrypts the certificate of authenticity to verify that the received second public key belongs to the second node. Upon such verification, the first node sends challenge data to the second node. The second node uses its private key to encrypt the challenge data before returning it to the first node. The first node uses the verified second public key to decrypt the encrypted challenge data received from the second node. If the decrypted challenge data matches the original challenge data, the first node sends a session key encrypted with the second public key to the second node for exchanging data. (Spec. 13-15, para. [0033]-[0037].)

Illustrative Claim

Independent claim 1 further illustrates the invention. It reads as follows:

1. A mobile ad-hoc network comprising:

Appeal 2008-2526
Application 10/197,148

a first node for generating an authentication request, said first node having a first public key and a first private key associated therewith; and

a second node having a second public key and a second private key associated therewith;

said first node receiving a certificate of authenticity responsive to the authentication request, the certificate of authenticity being generated by a certifying authority and comprising the second public key, the certifying authority having a public authentication key and a private authentication key associated therewith and generating the certificate of authenticity using the private authentication key;

said first node decrypting the certificate of authenticity using the public authentication key and verifying that the second public key belongs to said second node based upon the decrypted certificate of authenticity;

said first node sending challenge data to said second node upon verification that the second public key belongs to said second node;

said second node encrypting the challenge data using the second private key and returning the encrypted challenge data back to said first node;

said first node decrypting the encrypted challenge data using the verified second public key and authenticating said second node if the decryption of the encrypted challenge data yields the original challenge data;

said first node sending a session key encrypted with the second public key to said second node for use with subsequent data transfers therebetween upon authenticating said second node.

key encryption on a message hash digest rather than on the entire message itself to increase authentication speed. Thus, one of ordinary skill in the art would not find sufficient rationale to perform the additional authentication operation, such as the claimed challenge-response, in Nguyen since it would increase the length of the authentication process in the resulting Stallings-Nguyen's communications system where speed is critical among the different nodes. (App. Br. 9-11, Reply Br. 2.) Appellant therefore concludes that Nguyen teaches away from Stallings. (*Id.*)

Examiner's Findings/Conclusions

The Examiner finds that Stallings' disclosure of a sender using nonce values and the valid public key of a receiver to verify the identity of the receiver, and to then securely share a secret key with the receiver *substantially* teaches the challenge-response operation, as recited in independent claim 1. (Ans. 14.) Further, the Examiner recognizes that Nguyen discloses performing a public key encryption on a hash digest of a message, as opposed to encrypting the entire message, as a way to expedite the authentication process in the MANET. (Ans. 15.) However, the Examiner also finds that the MANET environment disclosed in Nguyen can be used for implementing the authentication process of the mobile nodes disclosed in Stallings. Therefore, the Examiner concludes that Stallings and Nguyen are properly combined to render claim 1 unpatentable. (*Id.*)

II. ISSUE

Did Appellant show the Examiner erred in concluding that the combination of Stallings and Nguyen renders the claimed invention unpatentable. Particularly, the issue turns on whether the ordinarily skilled artisan would have found sufficient rationale to combine the cited references to teach in a MANET (1) encrypting challenge data using a second private key at a second node, and (2) decrypting the challenge data using a second public key at a first node to thereby authenticate the second node if the original challenge data matches the decrypted challenge data, as recited in independent claim 1.

III. FINDINGS OF FACT

The following findings of fact (FF) are supported by a preponderance of the evidence.

Stallings

1a. As shown in Figure 6.12, Stallings discloses a communication network having a plurality of nodes including an initiator node A, a responder node B and a public key authority that are exchanging messages. (P. 184.)

1b. Particularly, node A submits to the public key authority a request for the current public key of node B. The authority uses its private key to encrypt a message, and transmits the encrypted message to node A. (P. 185.)

1c. Initiator A decrypts the message using the authority's public key. Node A then uses node B's public key to encrypt a message destined for node B. (*Id.*)

1d. Responder B retrieves node A's public key from the public key authority to decrypt node A's message, and to then encrypt a new response message including a nonce destined for initiator A. (*Id.*)

2. Stallings also discloses that both nodes A and B submit a public key and a certificate request to the certificate authority. In response, each of the nodes receives from the certificate authority the requested certificate along with the authority's public key. (P. 186.)

3a. Initiator node A uses responder node B's public key to encrypt a message destined for node B. The encrypted message includes a challenge nonce (N_1), and an identifier of node A to uniquely identify a particular transaction. (P. 188.)

3b. Upon receiving the encrypted message from initiator node A, responder node B decrypts it, and uses node A's public key to encrypt a response message including the challenge nonce (N_1) received from node A, as well as a new nonce (N_2) generated by node B. (P. 188.)

3c. Upon receiving the response message including the original nonce (N_1), node A can confirm that it originates from node B by using node B's public key to encrypt the new nonce (N_2), and subsequently return it to node B. (P. 189.)

3d. Node A then selects a secret key and uses it with a node B's public key to encrypt a message destined for node B such that only node B can decrypt it. (P. 189.)

Nguyen

4. Nguyen discloses a MANET having a plurality of nodes for securely exchanging messages with one another through public key encryption. Particularly, a signer encrypts the message with its private key, and sends the encrypted message to an intended recipient who decrypts it using the sender's public key. Nguyen discloses, however, that such public key encryption approach is relatively slow, and can take up a lot of space in an ad hoc network. (Para. 4.2.)

5. Alternatively, Nguyen discloses a one-way hash function scheme to remedy the space and speed constraints of the public key encryption approach. Particularly, Nguyen discloses using a one-way hash function with the public key encryption to provide an efficient digital signature. The sender can thus use the one-way hash function on the message, and then encrypt the hash value with his/her private key. The encrypted hash value and the message are then sent to the recipient who independently calculates another hash value on the message. Subsequently, the recipient decrypts the received hash value, and compares it with the calculated hash value to authenticate the user's signature if the two hash values match. (Para 4.2.)

IV. PRINCIPLES OF LAW

Obviousness

Appellant has the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1734 (2007).

In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," and discussed circumstances in which a patent might be determined to be obvious. *KSR*, 127 S. Ct. at 1739 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* The operative question in this "functional approach" is thus "whether the

improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 1740.

The Federal Circuit recently recognized that "[a]n obviousness determination is not the result of a rigid formula disassociated from the consideration of the facts of a case. Indeed, the common sense of those skilled in the art demonstrates why some combinations would have been obvious where others would not." *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007) (citing *KSR*, 127 S. Ct. 1727, 1739 (2007)). The Federal Circuit relied in part on the fact that Leapfrog had presented no evidence that the inclusion of a reader in the combined device was "uniquely challenging or difficult for one of ordinary skill in the art" or "represented an unobvious step over the prior art." *Id.* at 1162 (citing *KSR*, 127 S. Ct. at 1740-41).

One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art. *See In re Kahn*, 441 F.3d at 987-988 (Fed. Cir. 2006), *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991) and *In re Keller*, 642 F.2d 413, 425 (CCPA 1981). Moreover, in evaluating such references it is proper to take into account not only the specific teachings of the references but also the inferences which

one skilled in the art would reasonably be expected to draw therefrom. *In re Preda*, 401 F.2d 825, 826 (CCPA 1968).

V. ANALYSIS

Independent claim 1 recites in relevant part a MANET wherein a first mobile node and a second mobile node encrypt and decrypt received challenge-response data in order to authenticate the parties before they can be allowed to securely exchange data. As set forth in the Findings of Facts section, Stallings discloses a communications network having an initiator and a responder encrypting and decrypting nonce challenge data to authenticate the parties before they can share a secret key to exchange messages. (FF. 3a-3d.) We find that Stallings' disclosure reasonably teaches the challenge-response data between the first and second nodes as recited in independent claim 1. As noted above, the Examiner similarly finds that the disclosed nonce exchange between the parties teaches the claimed challenge-response. However, Appellant's arguments nowhere dispute such findings as advanced by the Examiner. Rather, Appellant's arguments focus on the combinability of Stallings' teachings with Nguyen's as being allegedly improper. While Nguyen does discuss the space and speed shortcomings of the public key encryption approach, it does recognize such approach as being known and widely used in the art. (FF. 4.) In other words, Nguyen does recognize the public key encryption approach as being an alternative encryption scheme, although it may not be as viable as the

Appeal 2008-2526
Application 10/197,148

one-way hash function encryption approach when it comes to enhancing speed and space in a MANET. (FF. 4-5.) We note nonetheless, it is offered as an alternative that is known to have been used in the MANET environment. Furthermore, we note that Appellant appears to have overlooked the fact that the Examiner only relies upon Nguyen for its teaching of providing the necessary environment for implementing the claimed MANET using the different nodes disclosed in Stallings. We therefore conclude that one of ordinary skill in the art would readily appreciate that Stallings and Nguyen disclose prior art elements that perform their ordinary functions to predictably result in a MANET that uses challenge-response nonce data to authenticate the mobile nodes thereon before they can be allowed to securely transfer exchange messages. We therefore do not agree with Appellant that the combination of Stallings and Nguyen is improper. For these same reasons, we do not agree with Appellant that Nguyen teaches away from Stallings.

Additionally, it is worth noting that the mobile ad hoc network (MANET) limitation is only recited in the preamble of the claim, and appears nowhere in the body of the claim. In general, a preamble is construed as a limitation “if it recites essential structure or steps, or if it is ‘necessary to give life, meaning, and vitality’ to the claim.” *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (quoting *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999)). A preamble is not limiting, however, “where a patentee

defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention.” *Id.* (quoting *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir. 1997)). *Symantec Corp. v. Computer Associates International Inc.*, 86 USPQ2d 1449, 1453-54 (Fed. Cir. 2008). We therefore find the mobile ad hoc network recitation to be a mere statement of intended use. We thus decline to give any patentable weight to the cited recitation. Consequently, we find that alternatively Stallings anticipates the claimed invention.

It follows that Appellant has not shown that the Examiner erred in concluding that the combination of Stallings and Nguyen renders claim 1 unpatentable.

Appellant did not provide separate arguments with respect to the rejections of claims 2 through 4, 6 through 24, 26, 27, 29 through 34, and 36 through 42. Consequently, these claims fall together with representative claim 1. 37 C.F.R. § 41.37(c)(1)(vii).

VI. CONCLUSIONS OF LAW

Appellant has not shown that the Examiner erred in concluding that the combination of:

1. Stallings and Nguyen renders claims 1-4, 6, 8-17, 19-24, 27, 29-34, 36, and 38-42 unpatentable under 35 U.S.C. § 103(a).
2. Stallings, Nguyen, and Hanson renders claims 7, 18, 26, and 37 unpatentable under 35 U.S.C. § 103(a).

Appeal 2008-2526
Application 10/197,148

VII. DECISION

We affirm the Examiner's decision to reject claims 1 through 4, 6 through 24, 26, 27, 29 through 34, and 36 through 42.

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

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO FL 32801