

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SCOTT P. DUBAL, DOUGLAS D. BOOM,
PATRICK L. CONNOR, and MARK V. MONTECALVO

Appeal 2008-4251
Application 10/323,985¹
Technology Center 2400

Decided: January 15, 2009

Before HOWARD B. BLANKENSHIP, JEAN R. HOMERE, and
CAROLYN D. THOMAS, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

¹ Filed on December 18, 2002. The real party in interest is Intel Corp.

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1 through 38. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

Appellants' Invention

Appellants invented a method and system for detecting attacks on a network. (Spec. 4.) As shown in Figure 8, the network includes a network adapter (200) that examines an incoming packet for possible threats. Upon detecting at least a characteristic of a denial of service (DOS) attack in the received packet, the network adapter blocks the packet from being processed at a host processor (106). (Spec. 9-10.)

Illustrative Claims

Independent claims 1 and 30 further illustrate the invention. They read as follows:

1. A method, comprising:

receiving at least one packet at a network adapter, the network adapter comprising a media access controller and logic to perform direct memory access (DMA) to a host memory and generate an interrupt to a host processor;

determining, at the network adapter, whether the at least one received packet has at least one characteristic of a denial of service attack; and

if it is determined that the at least one received packet has at least one characteristic of a denial of service attack, preventing, by the network adapter, processing of the at least one received packet by a transport layer protocol of a protocol stack.

30. A system comprising:
at least one host processor;
memory accessible by the at least one host processor;
at least one network adapter, comprising:
at least one physical layer (PHY) component;
at least one link layer component coupled to the at least one PHY component; and
logic to operate on packets received via the link layer component, initiate a direct memory access (DMA) transfer of data in the packets to the memory accessible by the at least one host processor, and generate an interrupt to the at least one host processor, the logic to:
receive at least one packet at a device;
determine whether the at least one received packet has at least one characteristic of a denial of service attack; and
if it is determined that the at least one received packet has at least one characteristic of a denial of service attack, prevent transfer of data included in the received packet to the host memory.

Appeal 2008-4251
Application 10/323,985

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

| | | |
|-------------|-----------------|---------------|
| Lachman | 2002/0166063 A1 | Nov. 7, 2002 |
| Tarquini | 2003/0084329 A1 | May 1, 2003 |
| Gulick | 2003/0097587 A1 | May 22, 2003 |
| Fretwell | 2003/0236995 A1 | Dec. 25, 2003 |
| Cox | 2004/0039940 A1 | Feb. 26, 2004 |
| Schulzrinne | 6,970,909 B2 | Nov. 29, 2005 |
| Carroll | 6,973,580 B1 | Dec. 6, 2005 |

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

1. Claims 1 through 4, and 10 through 12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lachman, Tarquini, and Schulzrinne.
2. Claims 5 through 9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lachman, Tarquini, Schulzrinne, and Fretwell.
3. Claims 13 and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lachman, Tarquini, Schulzrinne, and Carroll.
4. Claims 15 through 18, 24, 28, and 29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lachman, and Schulzrinne.

5. Claims 19 through 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lachman, Schulzrinne, and Fretwell.
6. Claims 25 through 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Lachman, Schulzrinne, and Carroll.
7. Claims 30 through 32, 35, and 37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Cox, Lachman, and Schulzrinne.
8. Claims 33 and 34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Cox, Lachman, Schulzrinne, and Fretwell.
9. Claim 36 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Cox, Lachman, Schulzrinne, and Carroll.
10. Claim 38 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Cox, Lachman, Schulzrinne, and Gulick.

Appellants' Contentions

Appellants argue that the combination of Lachman, Tarquini, and Schulzrinne does not render independent claim 1 unpatentable. (App. Br. 8-11.) Particularly, Appellants argue that while the cited references teach a DOS attack on a network, they are not properly combinable since Tarquini's

filtering of packets would undermine the method of operation of Lachman's system. That is, incorporating Tarquini's packet filtering scheme into Lachman's surveillance system would allegedly prevent an incoming packet from reaching Lachman's learning modules, thereby incapacitating the modules from learning the attack signatures of the incoming packet. (*Id.* at 9.)

Further, Appellants argue that the combination of Cox, Lachman, and Schulzrinne does not render independent claim 30 unpatentable. (*Id.* at 15-17.) Particularly, Appellants argue that Cox's processing of packets before they reach the host processor memory is contrary to Lachman's passive monitoring of packets. (*Id.* at 16.) Additionally, Appellants argue that Schulzrinne discloses an Ethernet controller for receiving and discarding incoming packets whereas Cox and Lachman describe monitoring attacks that occur higher in the protocol stack (e.g. transport layer or media access control layer). Appellants thus submit that the ordinarily skilled artisan would not have found sufficient rationale to migrate the lower layer operations of Schulzrinne into the higher layer operations of Cox and Lachman. (*Id.* at 17.)

Examiner's Findings/Conclusions

The Examiner finds that Lachman's disclosure of a network monitoring system that prevents undesired attacks from reaching a host server on the network *substantially* teaches the DOS attack detection

mechanism, as recited in independent claim 1. (Ans. 28.) Further, to complement Lachman, the Examiner relies upon Tarquini for its teaching of a three layered intrusion prevention system that provides network exploit detection at the transport layer level of a node. (*Id.* at 29.) Additionally, the Examiner relies upon an Ethernet controller disclosed in Schulzrinne to teach the claimed network adapter. (*Id.* at 31-32.) Consequently, the Examiner concludes that Lachman, Tarquini, and Schulzrinne are properly combined to render claim 1 unpatentable. (*Id.* at 32.)

Similarly, the Examiner concludes that Cox, Lachman and Schulzrinne are properly combined to render claim 30 unpatentable. Particularly, the Examiner finds that both Cox and Lachman disclose analogous systems for protecting nodes from harmful and unwanted attacks. (*Id.* at 35.) In addition, the Examiner finds that Schulzrinne's network adapter complements the Cox-Lachman combination to yield the claimed invention as recited in claim 30. (*Id.*)

II. ISSUES

1. Did Appellants show that the Examiner erred in concluding that the combination of Lachman, Tarquini, and Schulzrinne 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 the recitation of upon determining that a packet received at a network adapter contains a characteristic of a DOS attack,

preventing processing of the packet by a transport layer protocol of a protocol stack, as recited in independent claim 1.

2. Did Appellants show that the Examiner erred in concluding that the combination of Cox, Lachman and Schulzrinne 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 the recitation of upon determining that a packet received at a network adapter contains a characteristic of a DOS attack, preventing data in the packet from being transferred to a host memory, as recited in independent claim 30.

III. FINDINGS OF FACT

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

Lachman

1a. Lachman discloses an anti-network terrorism (A.N.T.) system for protecting a host network from flood type DOS attack. (Abstract.)

1b. Particularly, as shown in Figure 1, the host network (101) includes an A.N.T. surveillance system (106) that passively monitors data packets sent between a host router (104) and a host server (102). (¶¶ [0069]-[0070].)

1c. The A.N.T. (106) includes a plurality of modules (206, 210, 212, 214, 216, 218) for examining the nature of the monitored packets.

Upon determining that a monitored data packet contains a flood type DOS attack, the A.N.T. system blocks the packet to thereby prevent it from reaching the host server (102). (¶¶ [0070], [0073]-[0076].)

Tarquini

2a. Tarquini discloses a three-layered intrusion prevention system for detecting network exploits on the network and transport layers of a network node to thereby protect the node from unwanted and malicious intrusions.

2b. Particularly, Tarquini discloses an IPS transport service provider layer that provides network exploit detection at the transport layer level. It comprises layered service provider filters to facilitate socket level filtering of packets at a node of a network. (¶ [0041].)

Cox

3a. As shown in Figure 2, Cox discloses a data packet filtering accelerator processor (250) that operates in parallel with a host processor (240) to perform high speed data packet filtering on a network. (¶ [0031].)

3b. The host processor performs bulk data processing, and controls the accelerator processor by providing it with the necessary rules to parse and classify the packets thereby freeing the host processor from the overhead operations associated with its filtering operations. (*Id.*)

3c. As shown in Figure 6, the host processor accesses registers (640) and an instruction cache (630) via a bus interface (650), which may be coupled to a direct memory access (660). (¶ [0042].)

Schulzrinne

4a. As shown in Figure 4, Schulzrinne discloses a network appliance device (100) having an Ethernet controller subsystem (110) that interfaces with a data network. (Col. 8, ll. 11-15.)

4b. The Ethernet controller can take the form of a media access controller (MAC) for Ethernet to act as a gatekeeper for accepting and rejecting corrupted/unwanted data packets received from the Ethernet. (Col. 7, ll. 46-52.)

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.”

Appeal 2008-4251
Application 10/323,985

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. at 1739). 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 1741).

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; *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

Claims 1 through 14

Independent claim 1 recites in relevant part upon determining that a packet received at a network adapter contains a characteristic of a DOS attack, preventing the packet from being processed by a transport layer protocol of a protocol stack. As set forth in the Findings of Facts section, Lachman discloses an A.N.T. system for determining whether monitored data packets originating from a router in destination to a host server contain unwanted attacks. (FF. 1a-1b.) Upon determining that the monitored data packets contain malicious data, the A.N.T. blocks the packets from reaching the host server. (FF. 1c.) Further, Tarquini discloses a three layered filtering

system for filtering unwanted and harmful data packets at the transport layer of a network node. (FF. 2a-2b.) We find that Lachman's A.N.T. surveillance system, by protecting the host server from malicious packets, reasonably teaches a network adapter that determines whether an intercepted packet contains a DOS attack characteristic to thereby prevent the packet from being processed by the transport layer of the host server. Further, we agree with the Examiner that Tarquini's disclosure of filtering unwanted data at the transport layer of a node complements Lachman's A.N.T. surveillance system by allowing it to use the transport layer of a protocol stack to filter out unwanted packets.

Appellants acknowledge that both Lachman and Tarquini teach filtering DOS attacks. (App. Br. 8.) However, Appellants argue that Tarquini's filtering of the unwanted packets would impede the modules in Lachman's A.N.T. surveillance system from performing their intended functions. (*Id.* at 8-9.) We disagree. We find that all intercepted data packets are first processed in the A.N.T. surveillance system where the modules thereof determine whether or not to forward them to the host server. Consequently, by first processing the data packets in the A.N.T. surveillance system, the cited modules do have an opportunity to perform their intended functions. In our view, one of ordinary skill in the art would have found sufficient rationale to modify Lachman's ANT surveillance system by appending Tarquini's filtering module subsequently to Lachman's initial filtering of the data packets as a way to further reinforce the initial filtering

of unwanted data packets. In this particular instance, the suggested combination would in no way undermine the modules in Lachman's A.N.T. surveillance system. We therefore conclude that the ordinarily skilled artisan would readily appreciate that the combination of Lachman and Tarquini disclose prior art elements that perform their ordinary functions to predictably result in an A.N.T. surveillance system that filters out unwanted packets at the transport layer of a node.

It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Lachman, Tarquini and Schulzrinne renders independent claim 1 unpatentable.

Appellants did not provide separate arguments with respect to the rejections of claims 2 through 14. Consequently, these claims fall together with representative claim 1. 37 C.F.R. § 41.37(c)(1)(vii).

Claims 15 through 29

For this group of claims, Appellants merely reiterate for independent claim 15 the same arguments previously submitted in the brief for claim 1. (App. Br. 12-15.) We have already addressed these arguments, and we did not find them to be persuasive. It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Lachman and Schulzrinne renders independent claim 15 unpatentable.

Appellants did not provide separate arguments with respect to the rejections of claims 16 through 29. Consequently, these claims fall together with representative claim 15. 37 C.F.R. § 41.37(c)(1)(vii).

Claims 30 through 38

Independent claim 30 recites in relevant part upon determining that a packet received at a network adapter contains a characteristic of a DOS attack, preventing data in the packet from being transferred to a host memory. As set forth in the Findings of Facts section, Cox discloses a host processor and an accelerator processor that perform packet filtering in a parallel fashion. (FF. 3a-3c.) As discussed above, Lachman discloses an A.N.T. surveillance system for preventing unwanted data packets from reaching a host server. Additionally, Schulzrinne discloses an Ethernet controller that emulates a MAC to accept or reject data packets that arrive at a network node. (FF. 4a-4b.) We find that the ordinarily skilled artisan would readily recognize that Cox, Lachman and Schulzrinne disclose prior art elements that perform their ordinary functions to yield an A.N.T. surveillance system that uses numerous modules, an acceleration processor, a host processor, and an Ethernet controller to expeditiously and reliably filter unwanted data packets arriving at a node to thereby prevent them from being transferred to a host server. Therefore, we do not agree with Appellants that the combination is improper.

Appeal 2008-4251
Application 10/323,985

It follows that Appellants have not shown that the Examiner erred in concluding that the combination of Cox, Lachman, and Schulzrinne renders independent claim 30 unpatentable.

Appellants did not provide separate arguments with respect to the rejections of claims 31 through 38. Consequently, these claims fall together with representative claim 30. 37 C.F.R. § 41.37(c)(1)(vii).

VI. CONCLUSION OF LAW

Appellants have not shown that the Examiner erred in concluding that claims 1 through 38 are unpatentable as set forth above.

VII. DECISION

We affirm the Examiner's decision to reject claims 1 through 38.

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

msc

CAVEN & AGHEVLI
c/o INTELLEVATE, LLC
P.O. BOX 52050
MINNEAPOLIS MN 55402