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.
14/240,198	02/21/2014	Valiuddin Y. Ali	83786624	7054

22879 7590 02/04/2019

HP Inc.
3390 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528-9544

EXAMINER
WEI, ZENGPU

ART UNIT	PAPER NUMBER
2192	

NOTIFICATION DATE	DELIVERY MODE
02/04/2019	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):

ipa.mail@hp.com
barbl@hp.com
yvonne.bailey@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte VALIUDDIN Y. ALI, JOSE PAULO XAVIER PIRES, JAMES M. MANN, BORIS BALACHEFF, and CHRIS I. DALTON

Appeal 2018-004233
Application 14/240,198
Technology Center 2100

Before JOHN A. JEFFERY, LARRY J. HUME, and MATTHEW J. McNEILL, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants[1] appeal under 35 U.S.C. § 134(a) from the Examiner's decision to reject claims 1–4, 6–8, 10, 12–14, and 16–24. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

---

[1] Appellants identify the real party in interest as Hewlett-Packard Development Company, L.P. App. Br. 1.

STATEMENT OF THE CASE

Appellants' invention handles system management requests in a computing system by managing a trusted virtual machine (VM). In one aspect, all communications from a guest domain to a Basic Input/Output System (BIOS) are trapped and routed to a privileged domain portion for processing. *See generally* Abstract; Spec. ¶¶ 20–23, 26. Claim 7 is illustrative:

> 7. A method of handling a system management request in a computing system, comprising:
>
> managing, by a virtual machine monitor (VMM), a trusted virtual machine (VM) with a virtual high-privilege mode, the trusted VM with the virtual high-privilege mode to receive the system management request;
>
> preventing the system management request from initiating a system management mode at a processor of the computing system;
>
> handling the system management request by the trusted VM with the virtual high-privilege mode; and
>
> trapping, by the VMM, requests to a physical basic input/output system (BIOS) of the computing system from sources other than the trusted VM, the trapping of the requests preventing the requests from being communicated to the physical BIOS.

THE REJECTIONS

The Examiner rejected claims 1, 7, 8, 12, 16–20, and 22–24 under 35 U.S.C. § 103 as unpatentable over Neiger (US 7,581,219 B2; issued Aug. 25, 2009) and Aguilar (US 6,799,316 B1; issued Sept. 28, 2004). Final Act. 3–12.[2]

---

[2] Throughout this opinion, we refer to (1) the Final Rejection mailed May 16, 2017 ("Final Act."); (2) the Appeal Brief filed October 8, 2017 ("App.

The Examiner rejected claims 2–4 and 21 under 35 U.S.C. § 103 as unpatentable over Neiger, Aguilar, and Zimmer (US 2009/0172661 A1; published July 2, 2009). Final Act. 12–14.

The Examiner rejected claims 6, 10, and 14 under 35 U.S.C. § 103 as unpatentable over Neiger, Aguilar, and Sancho-Dominguez (US 2010/0199062 A1; published Aug. 5, 2010). Final Act. 14–17.

The Examiner rejected claim 13 under 35 U.S.C. § 103 as unpatentable over Neiger, Aguilar, and Franco (US 2013/0042003 A1; published Feb. 14, 2013). Final Act. 17–18.

THE OBVIOUSNESS REJECTION OVER NEIGER AND AGUILAR

The Examiner finds that Neiger discloses, among other things, a VMM that traps requests to a handler that controls access to system resources, thus preventing communicating the requests to those resources. *See* Final Act. 3–4; Ans. 5–6. Although the Examiner acknowledges that Neiger does not teach that the request is to a physical BIOS, the Examiner nonetheless finds that ordinarily skilled artisans would understand that system resources include BIOS as verified by Aguilar that is said to teach sending requests to physical BIOS via a system management interrupt (SMI) trap and handler. *See* Final Act. 4–5; Ans. 7. Based on these collective teachings, the Examiner concludes that the claim would have been obvious. *See* Final Act. 5; Ans. 5–7.

Appellants argue that because Neiger's sub-operating mode system mode system interrupt relied upon by the Examiner is a request sent to a

---

Br."); (3) the Examiner's Answer mailed January 16, 2018 ("Ans."); and (4) the Reply Brief filed March 13, 2018 ("Reply Br.").

VMM—not a physical BIOS—Neiger does not teach or suggest trapping requests to a physical BIOS to prevent communicating the requests to the BIOS as claimed. App. Br. 5–9; Reply Br. 3–5. Appellants add that the Examiner's reliance on Aguilar is also misplaced because even if Aguilar discloses a request to a BIOS, the request would actually be received by the BIOS contrary to the claimed invention that prevents such communication. App. Br. 9; Reply Br. 7.

ISSUE

Under § 103, has the Examiner erred by finding that Neiger and Aguilar collectively would have taught or suggested a VMM that traps requests to a physical BIOS, thus preventing communicating the requests to the BIOS as recited in claim 1?

ANALYSIS

On this record, we find the Examiner's rejection problematic essentially for the reasons indicated by Appellants. *See* App. Br. 5–10; Reply Br. 1–8. First, as the Examiner acknowledges (Ans. 4), Neiger is silent regarding trapping requests to a *physical BIOS*, let alone preventing communicating those requests to a BIOS. As shown in Neiger's Figure 1, VM domains 100 and 108 contain main VM monitor (MVMM) 101 and system management mode VM monitor (SVMM), respectively. *See* Neiger, col. 2, l. 63 – col. 3, l. 6; col. 3, l. 40 – col. 4, l. 5. Neiger explains that to permit limited sub-operating system mode code execution within a secure environment, the sub-operating system mode interrupt may be first directed *to a handler* in a trusted code module that controls VM access to system

resources. Neiger, col. 3, ll. 22–26. This routing of the interrupt *to the handler* may involve the trusted code to specify the location of the code used to service the interrupt. *Id.* col. 3, ll. 26–29. Then, the interrupt is directed to the sub-operating system mode code *in another VM monitor domain* to service the interrupt. *Id.* col. 3, ll. 30–34.

The clear import of this discussion is that Neiger's interrupt is sent to a handler—not BIOS. Nor is there persuasive evidence on this record to substantiate the Examiner's finding that Neiger's system resources to which VM access is controlled include BIOS. But even assuming, without deciding, that these system resources could somehow include BIOS as the Examiner indicates (Ans. 4), that does not mean that Neiger's interrupt-based request is sent *to* the BIOS. Rather, the request is directed *to a handler* in a trusted code module that *controls VM access to system resources*. Neiger, col. 3, ll. 22–26.

Our emphasis underscores that Neiger merely teaches controlling access to system resources—not sending the interrupt-based requests *to* those resources, let alone trapping those requests to prevent their communication to BIOS as claimed. To the extent that the Examiner finds that by controlling access to system resources, Neiger's handler somehow sends the received interrupt-based requests *to* those resources, including BIOS (*see* Ans. 5), such a finding is unsubstantiated on this record. Rather, as noted above, Neiger's interrupt-based requests are sent only to the handler.

Aguilar does not cure this deficiency. As shown in Aguilar's Figure 3, ROM BIOS 303 is connected to SMI trap 324 via bus 306. Aguilar, col. 5, l. 55 – col. 6, l. 6. Notably, the SMI handler is configured as

a software routine or utility *in the BIOS*, and receives the SMI from the trap. *Id.* col. 6, ll. 35–40. Because the *BIOS-based* handler receives the SMI, the BIOS receives interrupt-based requests: the very opposite of the claimed invention's trapping functionality that *prevents* communicating requests to the BIOS as Appellants indicate. App. Br. 9; Reply Br. 7.

Despite the apparently limited purpose for which Aguilar was cited, namely to "verify" that Neiger's system resources include BIOS (*see* Ans. 4), the cited prior art still does not teach or suggest a VMM that traps requests *to BIOS*, and thus prevent communicating those requests to the BIOS as claimed.

Therefore, we are persuaded that the Examiner erred in rejecting (1) independent claim 7; (2) independent claims 1 and 12 that recite commensurate limitations; and (3) dependent claims 8, 16–20, and 22–24 for similar reasons. Because this issue is dispositive regarding our reversing the Examiner's rejection of these claims, we need not address Appellants' other associated arguments.

THE REMAINING REJECTIONS

Because the Examiner has not shown that the cited prior art cures the foregoing deficiencies regarding the rejection of the independent claims, we will not sustain the obviousness rejections of dependent claims 2–4, 6, 10, 13, 14, and 21 (Final Act. 12–18) for similar reasons.

CONCLUSION

The Examiner erred in rejecting claims 1–4, 6–8, 10, 12–14, and 16–24 under § 103.

DECISION

We reverse the Examiner's decision to reject claims 1–4, 6–8, 10, 12–14, and 16–24.

REVERSED