

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

---

*Ex parte* ERIC J. RUFF and ROBERT S. RAYMOND

---

Appeal No. 2002-2176  
Application No. 08/948,931

---

ON BRIEF

---

Before BARRETT, BARRY, and LEVY, *Administrative Patent Judges*.  
BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

A patent examiner rejected claims 1, 3-9, 17-26, and 31-36. The appellants appeal therefrom under 35 U.S.C. § 134(a). We reverse.

BACKGROUND

The invention at issue on appeal detects and removes computer viruses. Computer viruses can cause unrecoverable errors, delete files, create intermittent problems, and otherwise cause frustration and damage. (Spec. at 1.) According to the appellants, a stealth virus hides its presence by altering the path between a computer's application programs and its storage media. In an IBM-compatible computer using the

MS-DOS® operating system, for example, requests by an application program to read a diskette are serviced by a Basic Input/Output System ("BIOS").<sup>1</sup> (*Id.* at 7.) To hide its presence, a stealth virus may install itself in the BIOS' Master Boot Record ("MBR")<sup>2</sup> and modify attempts to read the MBR. The virus may also create a copy or "facade" of the original, uninfected MBR. (*Id.* at 4.) Attempts to check the integrity of the MBR via checksums or data values, explain the appellant, are then intercepted by the virus and performed on the copy instead of the infected MBR. The virus thus evades detection. (*Id.* at 4-5.)

In contrast, the appellants' invention uses an alternate BIOS to detect and remove viruses. Unlike the standard BIOS, they assert, the alternate BIOS is trusted because it has been "kept inaccessible to viruses." (*Id.* at 8.) Viruses can be detected, the appellants add, by noting any difference between results obtained using the standard, possibly infected BIOS and the uninfected, alternate BIOS. (*Id.* at 7.) The invention also relocates facades to their proper location. (*Id.* at 8.)

---

<sup>1</sup>The BIOS enables a programmer to operate a disk drive without acquiring an exhaustive knowledge of the specific brand of drive hardware being used. The BIOS is typically stored in a read-only memory chip. (Spec. at 2-3.)

<sup>2</sup>The MBR contains a disk boot program that will load operating system code and eventually pass control to a command interpreter or other user interface. (Spec. at 3.)

A further understanding of the invention can be achieved by reading the following claim.

1. A computer system comprising:

a storage subsystem including a storage medium and a controller, the controller having a controller interface for controlling access to the storage medium;

a virus target structure stored on the storage medium;

a translation means for translating between logical requests for access to the storage medium and corresponding parameters used in the controller interface; and

a detection means for detecting a virus using an alternate path to the storage medium by detecting alteration of the correspondence between logical requests for access to the virus target structure and the corresponding controller interface parameters.

Claims 1, 3-9, 17-26, and 31-36 stand rejected under 35 U.S.C. § 103(a) as obvious over IBM Technical Disclosure Bulletin, *Artificial Immunity for Personal Computers*, vol. 34, no. 2 (July 1991) ("TDB") and U.S. Patent No. 5,881,151 ("Yamamoto").

## OPINION

Rather than reiterate the positions of the examiner or the appellants *in toto*, we address the main point of contention therebetween. The examiner makes the following assertions.

TDB clearly teaches that the virus detector [ISP] has direct access to the I/O device [disk drive] and the controller thereof [disk drive controller]. TDB teaches the generic use of ISP to detect virus. TDB fails to teach what specific parameter from the disk drive is to be used to detect virus. Yamamoto teaches the usage of the disk address to detect virus. Yamamoto is silent about the source of the detected disk address. As such, Yamamoto's teaching of the source of the detected disk address encompasses all sources of the detected disk address. In the IBM TDB - Yamamoto system, the disk address is coming from the disk controller because IBM TDB has direct access to the disk drive controller.

(Examiner's Answer, § 12.<sup>3</sup>) The appellants argue, "disk addresses are not controller interface parameters." (Reply Br. at 3.) They add, "Yamamoto does not even discuss 'controller', 'interface', or 'register'. The asserted grounds for rejection fail to bridge the gap between comparing the disk address of an object program and comparing controller register values for an MBR as discussed in the application." (*Id.*)

In addressing the point of contention, the Board conducts a two-step analysis. First, we construe claims at issue to determine their scope. Second, we determine whether the construed claims would have been obvious.

---

<sup>3</sup>The examiner should number the pages of his answers.

## 1. CLAIM CONSTRUCTION

"Analysis begins with a key legal question -- *what* is the invention *claimed*?"

*Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1567, 1 USPQ2d 1593, 1597 (Fed. Cir. 1987). In answering the question, "[c]laims are not interpreted in a vacuum, but are part of and are read in light of the specification." *Slimfold Mfg. Co. v. Kinkead Indus., Inc.*, 810 F.2d 1113, 1116, 1 USPQ2d 1563, 1566 (Fed. Cir. 1987) (citing *Hybritech Inc. v. Monoclonal Anti-bodies, Inc.*, 802 F.2d 1367, 1385, 231 USPQ 81, 94-95 (Fed. Cir. 1986); *In re Mattison*, 509 F.2d 563, 565, 184 USPQ 484, 486 (CCPA 1975)).

Here, claim 1 recites in pertinent part the following limitations: "detecting a virus using an alternate path to the storage medium by detecting alteration of the correspondence between logical requests for access to the virus target structure and the corresponding controller interface parameters." Claims 18 and 31 include similar limitations.

The appellants' specification describes the "detecting a virus" as follows.

One search method includes an attempted target reading step 412, an alternate target reading step 414, and a data comparing step 416. During the attempted target reading step 412, the virus detector 312 reads the Master Boot Record or other target using the native BIOS 304 and/or the operating system 302. During the alternate target reading step 414, the virus detector 312 uses the detector's private BIOS 314 to read the same target. The data resulting from the two reads is then compared during the step 416.

If the regular BIOS 304 and the alternate BIOS 314 produce the same data, and if that data is what would be expected in an uninfected system, then the target is probably not infected. On the other hand, suppose the regular BIOS 304 produces the data expected in an uninfected system but the alternate BIOS 314 does not. . . . [T]hen the target is probably infected; the regular BIOS 304 calls were probably redirected to a facade copy of the target data by a stealth virus which has just now been revealed by the invention.

(Spec. at 18-19.) Reading the limitations in light of the specification, claims 1, 18, and 31 require using a native BIOS or an operating system to read a target of a virus, using a virus detector's private BIOS to read the same target, and comparing data resulting from the two reads.

## 2. OBVIOUSNESS DETERMINATION

Having determined what subject matter is being claimed, the next inquiry is whether the subject matter would have been obvious. "In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993) (citing *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)). "A *prima facie* case of obviousness is established when the teachings from the prior art itself would . . . have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Bell*, 991 F.2d 781, 783, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976)).

Here, admitting that "TDB fails to teach [the claimed] detecting a virus," (Examiner's Answer, § 10), the examiner cites to "col. 9, lines 30-55" of Yamamoto to teach the limitations. (*Id.*) That passage includes the following disclosure.

When the virus diagnosing mechanism 18 has received an activation input during the execution of the object program having the virus diagnosing mechanism 18 embedded therein, the disk address detection portion 84 detects the disk address that has been written at this time, for example, the volume No., the file No. and the track address to send the disk address to the disk address comparison portion 86. The disk address comparison portion 86 reads, from the original disk address storage portion 88, the volume No. 90, the file No. 92 and the track address 94 as the original information to subject them to a comparison with detected information supplied from the disk address detection portion 84. If the detected information and the original information coincide with each other, the disk address comparison portion 86 discriminates that no virus infection takes place and generates a continuous output for continuing the object program. If the detected information and the original information do not coincide with each other, the disk address comparison portion 86 discriminates that a portion of the disk address has been broken due to virus infection and generates an interruption output.

Col. 9, ll. 26-47. Although the reference compares "detected information" and "original information," we are unpersuaded that the information results from using a native BIOS or an operating system to read a target of a virus and using a virus detector's private BIOS to read the same target. Absent a teaching or suggestion of using a native BIOS or an operating system to read a target of a virus, using a virus detector's private BIOS to read the same target, and comparing data resulting from the two reads, we are unpersuaded of a *prima facie* case of obviousness. Therefore, we reverse the obviousness rejection of claim 1; of claims 3-17 and 17, which depend therefrom; of

claim 18; of claims 19-26, which depend therefrom; of claim 31; and of claims 32-36, which depend therefrom.

#### CONCLUSION

In summary, the rejection of claims 1, 3-9, 17-26, and 31-36 under § 103(a) is reversed.

REVERSED

LEE E. BARRETT  
Administrative Patent Judge

LANCE LEONARD BARRY  
Administrative Patent Judge

STUART S. LEVY  
Administrative Patent Judge

)  
)  
)  
)  
)  
) BOARD OF PATENT  
) APPEALS  
) AND  
) INTERFERENCES  
)  
)  
)  
)

Appeal No. 2002-2176  
Application No. 08/948,931

Page 10

JOHN W. L. OGILVIE  
1320 EAST LAIRD AVENUE  
SALT LAKE CITY, UT 84105