BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN DES BREVETS

Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 26 February 2019

Case Number:	T 1719/17 - 3.5.06
Application Number:	06110963.3
Publication Number:	1701259
IPC:	G06F9/455, G06F9/46
Language of the proceedings:	EN

Title of invention:
Systems and methods for multi-level intercept processing in a virtual machine environment

Applicant:
Microsoft Technology Licensing, LLC

Headword:
Intercept processing/MICROSOFT

Relevant legal provisions:
EPC 1973 Art. 56, 83

Keyword:
Inventive step (no)
Sufficiency of disclosure (yes)

Decisions cited:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1719/17 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 26 February 2019

Appellant:
(Applicant)

Microsoft Technology Licensing, LLC
One Microsoft Way
Redmond, WA 98052 (US)

Representative:

Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München (DE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 27 March 2017 refusing European patent application No. 06110963.3 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller A. Teale

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, dated 27 March 2017, to refuse European patent application No. 06 110 963 for lack of compliance with Article 83 EPC (1973). Three documents were also cited, but their disclosure was only referred to cursorily in a section entitled "Further Remarks".

II. An appeal was filed on 18 May 2017, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 13 July 2017. The appellant requested that the decision be set aside and that a patent be granted on the basis of claims 1 to 13 according to a main request or one of two auxiliary requests as filed on 5 January 2017.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention complied with Article 83 EPC 1973 but not with Article 56 EPC 1973. Objections under Article 84 EPC 1973 were also raised.

IV. In response to the summons, with a letter dated 17 January 2019, the appellant filed amended claims according to a main and two auxiliary requests.

Claim 1 of the main request reads as follows:

"A method for processing intercepts for partitions (508, 510) in a virtual machine environment, said virtual machine environment comprising a virtualizer (504) and a partition, comprising:

transferring (604) control, from a guest operating system running in the partition, to the virtualizer, the transfer being caused by an event in the partition triggering an intercept;

forwarding (610), by said virtualizer, the intercept to a first external monitor (562, 564) running in the partition;

handling (616) the intercept by said first external monitor; and

returning (618) the control to the source of the intercept when intercept handling is complete, wherein the source of the intercept is the guest operating system running in the partition."

Claim 1 of auxiliary request 1 differs from that of the main request in that the "handling" step is replaced by the following steps:

"... determining (612), by the first external monitor, whether to handle the intercept by the first external monitor;

if the first external monitor determines to handle the intercept, handling (616) the intercept by said first external monitor;

if the first external monitor determines not to handle the intercept, returning the intercept to the virtualizer, requesting (614) the virtualizer to handle the intercept and handling (608) the intercept by the virtualizer; ..."

Claim 1 of auxiliary request 2 differs from that of auxiliary request 1 in setting out that the guest OS and the external monitor run in different, first and second partitions, respectively.

V. With the letter of 17 January 2019, the appellant also filed two documents published after the filing date of the present application ("USB Fuzzing for the Masses", 14 July 2011, downloaded by the appellant from labs.mwrinfosecurity.com/blog/usb-fuzzing-for-the-masses, and King S T *et al.*, "Designing and implementing malicious hardware" without a publication date, but apparently published in the proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, LEET'08, by the Usenix Association Berkeley, 2008; see https://www.usenix.org/legacy/event/leet08/tech/full_papers/king/king.pdf), in order to establish that the claimed invention improves security (see the letter, page 2, penultimate paragraph, to page 3, paragraph 1).

VI. Oral proceedings were held on 26 February 2019. At their conclusion, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application relates to intercept handling in the context of virtual machines.

1.1 A "virtual machine" (VM) is a "pure software representation of the operation of one specific hardware architecture", which allows a "guest operating system" (guest OS), developed for some specific hardware, to run on different hardware, the "host computer system" (see paragraphs 5 and 6).

1.2 The guest OS executes instructions targeted at the hardware for which it was developed (see, for example, claim 2 of the main request). That hardware not being present, these instructions may have to be "intercepted" so that what the targeted hardware "would have done" is "emulated" in software. Thus the "guest computer system" exists as a "virtual" construct, which is said to "fool the guest OS into thinking that it owns all the resources of the machine" (see paragraph 10). The fact that the "virtual machine" is "hardware that does not actually exist" (paragraph 28) is indicated by broken lines around the VM in the figures (see e.g. figure 2, no. 96, or figure 3A, nos. 108 and 110).

1.3 The software responsible for the intercepts and for mimicking the "guest computer system" is called a "virtual machine monitor" (VMM), "hypervisor" or "emulator", or, more generally, a "virtualizer" (see paragraphs 7-9 and 28; figure 2, no. 94). It is possible for a single "virtualizer" to deal with several "virtual machines" at the same time. These are referred to as "instances" of a VM or "partitions" (see paragraph 10, line 3, and figures 3A, 3B and 4).

1.4 The application states that a single, centralized ("monolithic") virtualizer tends to become too complex (paragraphs 10 and 38; fig. 4, no. 404) and proposes to simplify it with a "multi-level virtualizer" (see paragraph 11). The basic idea is that, in tandem with a slim central "base-level" virtualizer (figure 5, no. 504; par. 40), separate "external monitors" (EMs), one per "partition", "resolve[s] the intercepts" (still paragraph 11, and figure 5, nos. 562 and 564). More specifically, it is disclosed that the intercepts are first passed to the base-level virtualizer and either handled there or forwarded to an external monitor, which, in turn, may handle the intercept or return it to the base-level virtualizer to handle it after all (see paragraph 43).

1.5 The external monitors are said to "run" or "exist within a partition" (see paragraphs 11 and 40), whilst the partition is defined as "an individual instance of a VM" (see paragraph 10). Elsewhere it is stated that "external monitors can be registered with the virtualizer for each partition" (see paragraph 44). It is stressed that the external monitor corresponding to a VM, a partition, may have to "run within another partition" (see paragraph 45).

Claim construction

2. The invention which the application, according to Article 83 EPC 1973, must disclose in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art, is the subject-matter of the claims understood in the light of the description. Hence, that subject-matter must first be construed.

2.1 The description uses the term "instance of a virtual machine" and "partition" synonymously (see e.g. paragraphs 1, 10, 34). Each partition provides the guest OS and the external monitor running in it with certain resources which may or may not correspond to actual physical resources (see paragraph 34). As an example it is disclosed that a partition may be provided with merely one of four physical processors (*loc. cit.*). In principle, however, the inverse is also possible: software running in a partition may be "fooled into believing" that there are several processors where, in fact, there is only one. In addition, it is disclosed, although not claimed, that the virtualizer "exists near the kernel level of a" host operating system "HOS", whereas software in a partition runs "at guest level" (see paragraphs 8 and 40). The board thus takes the claimed term "partition", to the appellant's benefit, to imply virtualized resources and restricted access permissions when compared to the base level virtualizer.

2.2 Intercepts are primarily "events that occur while software is executing on a guest operating system in a partition" and which represents an "interaction that occurs between some component of the partition and some resource, physical or virtual, that is not in fact part of the partition", e.g. a "peripheral device" (see paragraph 10).

2.3 The claims specify that an "external monitor" - understood to be "external" in the sense of not being part of the virtualizer" - receives the intercept, handles it and "return[s]" control afterwards. The description uses the formulation that external monitors carry out "intercept-related functionality" (see paragraph 11). The board thus interprets the external monitor as a program which is distinct from the program implementing the virtualizer, but which functionally is part of the virtualizer in that it carries out functions which, in the prior art, would have been carried out by the "monolithic" virtualizer. It is not claimed or disclosed, however, what exactly the external monitors do.

Article 83 EPC 1973

3. The board sees no reason why the skilled person would be unable to carry out the claimed invention. Any code

split off from the monolithic virtualizer into external monitors can, in principle and with straightforward modifications, be run "like" a guest OS "in a partition", provided it can manage with the virtual resources and limited access privileges available in that partition. Although the board takes the point made by the examining division that running additional code within the same partition as a guest OS might destroy (or at least affect) the "illusion" created by the VM (see point 3.20 of the decision under appeal), this is not, in the board's judgment, a deficiency under Article 83 EPC 1973.

The prior art

4. The board considers that it was known in the art at the priority date, at least in broad terms, what it means to "process intercepts" in a "partition" - i.e. in an "instance of a VM" -, that "control" is "transferred" from a guest OS to the virtualizer, that the intercept is "handled", and that control is then returned to the "source of the intercept", in particular to the guest OS. This is, effectively, the scenario depicted in and described with reference to figure 4, which the application itself discloses as prior art (see paragraph 38). Beyond that, a detailed discussion of the prior art documents mentioned in the decision under appeal is not necessary for the purposes of the present decision.

Article 56 EPC 1973

5. Compared with the prior art, the invention is that some undefined "intercept-related functionality" is not carried out in the virtualizer but in a piece of software called an "external monitor" running in a

partition (see also figures 5 and 6). According to the main request and auxiliary request 1, the partition is the same as that of the guest OS triggering the intercept. According to auxiliary request 2, it is a different one.

6. The board is unable to discern the technical effect, if any, that this difference has over the whole range of the claimed subject-matter.

6.1 The appellant argues that the invention provides a simpler virtualizer (see the grounds of appeal, section 1.2, paragraph 3). The board considers it to be plausible that external monitors simplify the virtualizer if they relieve the virtualizer of handling an intercept (see claim 1 of the main request), or at least of having to carry out at least some "intercept-related functionality", but it is questionable when the virtualizer must still be able to handle all intercepts, because they might be returned by the external monitor (see claim 1 of auxiliary requests 1 and 2, and figure 6). Nevertheless the description discloses that the virtualizer might be able to handle an intercept in a "default" manner and the external monitor in a different way (see paragraph 43). If, for some reason, alternative handlers were required, one might consider it a simplification to limit the virtualizer to the "default" handling. In view of this, the board accepts that the external monitors simplify the base level virtualizer.

6.2 The appellant also argues that "the technical effect of running the external monitor 'in a partition'" is that it "improves 1) the performance, 2) the reliability and

3) the security of the system" (see the letter of 17 January 2019, page 2, paragraph 2).

6.2.1 In general, the external monitors do not - and are not intended to - change the effect of virtualization. In other words, the guest OSs and their associated applications should not normally notice any change due to the use of external monitors. Also, virtualization will not require fewer resources such as memory or computing time. If anything, the additional communication requirement between the external monitors and the virtualizer will increase the resource consumption. Also, in comparison to a monolithic virtualizer, the external monitors cannot be said to avoid "costly context transitions" (see the letter of 17 January 2019, page 2, paragraph 3). The board therefore does not accept that the claimed invention increases performance.

6.2.2 Increased security due to the use of external monitors is not explicitly discussed in the application. Apparently, if partitions provide fewer ("guest-level") privileges than the base level virtualizer has ("kernel-level"), then the external monitor can do less harm in a partition. But this is an immediate consequence of the fact that it can do less. As mentioned above (point 3), any functionality from the virtualizer that happens not to require other resources or privileges than those provided in a partition can be executed by an external monitor in that partition, and any other functionality cannot without compromising the entire virtualizer. The claims and description do not discuss how the functionality of the external monitors is determined in view of the resources or privileges in the partitions or how the decision is taken in which partition to run a particular external monitor in view of the requirements of the handler functionality. Also the precise circumstances under which running external monitors in partitions addresses the risk of "malicious hardware" is not discussed in the application or implied by the claim language. As the post-published documents filed with the letter of 17 January 2019 do not, therefore, help to illustrate a point that was disclosed, explicitly or implicitly, in the application as originally filed, no further reference need be made to them. Also, during the oral proceedings, the appellant did not refer to these documents to support its arguments.

6.2.3 Increased reliability is said to follow from the fact that run-time errors of external monitors can be contained in a partition (see the letter of 17 January 2019, page 2, paragraph 4). The board accepts that this effect exists but notes that it is not discussed in the application.

6.2.4 Finally, and with regard to auxiliary request 2, it is noted that the description mentions that handling an intercept in a different partition from that of the guest OS triggering the intercept might "prevent circular dependencies and deadlock situations" (see paragraph 45). The description does not, however, illustrate which circular dependencies or which deadlock situations could occur and in which circumstances. Hence it cannot be assessed whether the separation of guest OS and external monitor actually solves this problem.

7. In view of the above, the board considers that provision of the external monitors reduces the complexity of the base-level virtualizer and that

running the external monitors with reduced privileges increases reliability and security by limiting the potential harm they can cause. The effect of running the external monitors in one or another partition - i.e. with one or another specific set of virtual resources - is unclear in general, and specific circumstances in which this might have an advantage are neither claimed nor disclosed.

7.1 The board considers that the separation of certain software modules from a complex piece of software, external monitors from the virtualizer in the present case, is an obvious instance of modular programming which might, for instance, not serve any other purpose than to simplify the program development because, for instance, different external monitors can be developed independently and by different vendors. Whether this is a technical effect at all may be left open because the board considers it a standard measure in program development and thus to be obvious either way.

7.2 Moreover, the board judges it to be an obvious measure to increase security and reliability to provide any program module with only those privileges that it needs to do its job. Accordingly, it would be obvious to run an external monitor with only guest privileges if it happens not to need more than that.

7.3 As discussed above, it is not apparent what technical problem is solved by running the external monitors with the virtual resources of a partition rather than with the actual physical resources like the virtualizer. This feature can therefore not be taken into account when assessing inventive step.

7.4 In summary, the board concludes that claim 1 of all three pending requests lacks inventive step, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

Beschwerdekammern
des Europäischen Patentamts
Boards of Appeal
of the European Patent Office
Chambres de recours
de l'Office européen des brevets

L. Stridde W. Sekretaruk

Decision electronically authenticated