Internal distribution code:

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

Datasheet for the decision of 14 March 2024

Case Number: T 1887/19 - 3.5.06

Application Number: 08725870.3

Publication Number: 2126687

IPC: G06F9/06, G06F9/445

Language of the proceedings: EN

Title of invention:
METHODS AND SYSTEMS TO SELECTIVELY SCRUB A SYSTEM MEMORY

Applicant:
Hewlett-Packard Development Company, L.P.

Headword:
Memory scrubbing/HEWLETT-PACKARD

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (no)

Decisions cited:

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 1887/19 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 14 March 2024

Appellant: (Applicant)	Hewlett-Packard Development Company, L.P. 10300 Energy Drive Spring, TX 77389 (US)
Representative:	Hoffmann Eitle Patent- und Rechtsanwälte PartmbB Arabellastraße 30 81925 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 20 December 2018 refusing European patent application No. 08725870.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	S. Krischer
	A. Jimenez

Summary of Facts and Submissions

I. The appeal is directed against the decision of the examining division, dated 20 December 2018, to refuse application No. 08725870.3 for added subject-matter, lack of clarity and lack of inventive step over document D3 (US 2003/196100 A1).

II. A notice of appeal was received on 11 January 2019. The appeal fee was paid the same day. A statement of grounds of appeal was received on 15 April 2019 with which claims according to a main request and two auxiliary requests were filed.

III. In a communication dated 1 February 2024, the board gave reasons for its preliminary opinion that claim 1 of all of the requests lacked an inventive step over D3 and introduced a document to illustrate the technical background:

D7: TCG, "TCG Platform Reset Attack Mitigation Specification", 15 May 2008, available at https://www.trustedcomputinggroup.org/wp-content/uploads/Platform-Reset-Attack-Mitigation-Specification.pdf, accessed on 24 January 2024.

IV. In a letter dated 7 March 2024, the appellant submitted further arguments.

V. Oral proceedings were held on 14 March 2024. At their end, the board announced its decision.

VI. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1-6 according to the main request, subject of

the appealed decision, filed on 9 November 2018 and re-filed with the statement of grounds of appeal, or claims 1-4 according to auxiliary requests 1 or 2, filed with the statement of grounds of appeal. The other application documents are the same as indicated in the appealed decision.

VII. Claim 1 of the main request reads as follows:

"1. A computer system (100), comprising:
a processor (104);
a system memory (108) coupled to the processor (104);
a BIOS (130) in communication with the processor (104);
an I/0 bridge (112) coupled to the processor (104); and
an OS (142) in communication with the processor (104),
wherein the I/O bridge (112) is arranged to trap a shutdown request and cause the system (100) to enter an System Management Mode on the basis of a selection, the BIOS (130) being operative to scrub the system memory (108) in said System Management Mode during a shutdown process of the computer system (100) and scrubs the system memory (108) before the shutdown request is complete,
wherein the selection comprises the OS (142) setting a MOR bit (206) that causes the BIOS (130) to scrub the system memory (108) during a boot process of the computer system (100),
wherein the OS (142) is to clear the MOR bit (206) if at least one of the following occurs:
- a secret is deleted from a confidential area of the memory (108), and

- an OS security is disabled."

VIII. Claim 1 of auxiliary request 1 differs from that of the main request in that the paragraphs starting with "wherein" read:

"wherein the BIOS (130) is configured to scrub the system memory (108) during a shutdown process of the computer system (100),

wherein the OS (142) is configured to set a memory override, MOR, bit that causes the BIOS (130) to scrub the system memory (108) during a boot process of the computer system (100),

wherein the I/O bridge (112) is configured to trap a shutdown request and to cause the system (100) to enter an [sic] System Management Mode so that the BIOS (130) can scrub the system memory (108) during the shutdown process, wherein the BIOS (130) is configured to clear the MOR bit during a System Management Mode operation during the shutdown process."

IX. Claim 1 of auxiliary request 2 differs from that of auxiliary request 1 in that the order of occurrence of the I/0 bridge and the OS in the claim is reversed, and the last paragraph starting with "wherein" reads (additions are underlined):

"wherein the BIOS (130) is configured to clear the MOR bit (206) during a System Management Mode operation during the shutdown process, in response to a secret being deleted from the confidential area (110) of the system memory (108) while OS security is enabled."

Reasons for the Decision

1. The application relates to "scrubbing" the (system) memory (figure 1: 108) of a computer, i.e. deleting its contents, during its *shutdown* and clearing the MOR (Memory Overwrite Request) bit of the operating system in order to prevent an unnecessary further memory scrubbing during the subsequent *boot* process (original description paragraph [11], sentence 4). It is noted that the description also discloses the opposite ([32], last sentence: scrubbing during both, shutdown *and* subsequent boot even though the MOR bit is cleared). The MOR bit can be stored in the BIOS memory (Basic Input/Output System; see [22], sentence 1; see 130 in figure 1 for the BIOS), usually a non-volatile Flash memory. The invention is situated in the context of a TCG (Trusted Computing Group) compliant computer. The TCG has specified the concept of the MOR bit, which signals the BIOS to scrub the system memory (figure 1: 108, e.g. RAM) during a *boot* process to ensure that secrets (e.g. encryption keys or passwords) stored in RAM are deleted ([1], [12]). This is to protect the computer against reset or power cycle attacks ([2], sentence 1).

1.1 Regarding the reason why it is worth the effort to scrub a RAM during the boot process when its content is anyhow gone after shutdown, the TCG specification introduced as D7 (see above) explains the following (page 5, first paragraph):

> "When a [computer] reboots or shuts down, the contents of volatile memory (RAM) are not immediately lost. Without an electric charge to maintain the data in memory, the data will begin to

decay. During this period, there is a short timeframe during which an attacker can turn off or reboot the computer, and quickly turn it back on to boot into a program that dumps the contents of the memory. Encryption keys and other secrets can be compromised through this method."

1.2 According to the invention, the shutdown request (e.g. sent by the keyboard) is received and trapped by an I/O bridge (figure 1: 112) which notifies the BIOS by switching the computer into an SMM (System Management Mode), a mode from which the BIOS subroutines (e.g. for scrubbing the *entire* memory, figure 1: 134; or for clearing the MOR bit; see [24] for both, scrubbing and clearing) can be accessed without involvement of the OS ([16], sentences 3-6; [23], sentence 4).

1.3 The OS of the computer in question is said to "comprise[] a secure OS that supports the MOR bit" and that can be enabled or disabled ([20]). Further details about the functions provided by "OS security" or how it is "enabled" or "disabled" are not disclosed. Nor is it disclosed what it means for the "secure OS" to "support[] the MOR bit". An aspect of that "support" seems to be that the MOR bit may be set if "the OS security is enabled" and may be cleared if the the OS security [is] disabled" ([30]). However, it is also disclosed that the MOR bit may "remain set regardless of whether a secret has been stored in or cleared from the confidential area" ([20]), that "the BIOS 130 may clear the MOR bit even if OS security is enabled" ([24]) or "while" OS security is enabled" when ("in other words") the OS has not cleared the MOR bit ([31]).

2. As explained in its preliminary opinion, the board tended not to have any objections to the present sets of claims regarding added subject-matter (Article 123(2) EPC). However, this question did not have to be decided upon.

3. Regarding clarity and claim interpretation, the board makes the following observations.

3.1 Paragraph [30] supports the feature that the MOR bit is cleared if "a secret is deleted from a confidential area of the memory". This feature is also clear, even though the examining division was correct to note (see the decision, section 3.2.1) that "further secrets might be present" so that it appears dubious to clear the MOR bit if only "a" - i.e. one - secret is deleted.

3.2 With regard to section 3.2.2 of the decision, an MOR bit can be cleared even if it is not set. That this admittedly would be redundant does not make the claim unclear. Likewise, that the invention might not be protected against a specific attack (such as a reset attack as explained by the examining division in section 3.2.2) does not contravene Article 84 EPC.

3.3 The claims state that setting the MOR bit "causes the BIOS [...] to scrub the memory [...] during a boot process" although the MOR bit might be cleared before booting, in which case arguably its setting will not have "caused" anything (see the decision, section 3.2.3). The board interprets the cited clause as specifying a bit and a compliant BIOS so that, when the bit is set at boot time, the BIOS scrubs the memory.

3.4 The claims refer to an "MOR bit" and specify its intended function but do not otherwise refer to TCG compliance. The board therefore takes the view that the MOR bit must be construed as any bit with the specified function, regardless of what else TCG compliance might also imply on the MOR bit, the BIOS or the overall computer system. At this point, the board also notes that "TCG compliance" is in itself a dubious criterion in the present case. As the invention is expressly meant to improve the TCG standard as regards the handling of the MOR bit, it appears questionable to consider the invention to be TCG compliant in this sense. Beyond that, it would be unclear how exactly any reference to the TCG standard would limit the claims, as it contains quite a few details, many of which have no bearing on the claimed matter.

3.5 The claims refers to "a System Management Mode" without otherwise defining it, and specifically without requiring the processor to be of the x86 family in which that mode would have a special meaning. Accordingly, the claim must be interpreted as requiring a processor with some mode that has the properties claimed for the SMM. Which are only that the system, once a shutdown request is trapped, enters the mode and that the BIOS can, in this mode, scrub the memory.

4. As regards inventive step of claim 1 of the main request, the statement of grounds of appeal argues that, in addition to the difference between the claimed subject-matter and D3, which was recognized in the appealed decision (page 7), there are three further differences (U1-U3; see pages 10-11 of the statement of grounds).

4.1 These differences are, in the order in which they appear in the claim:

(U3) the BIOS scrubs system memory during shutdown in an SMM after having trapped a shutdown request;
(U1) the OS sets an MOR bit to signal scrubbing during booting;
(U2) the OS clears the MOR bit if a secret is deleted or OS security is disabled.

4.2 The first difference (U3) does not depend on the MOR bit and is therefore independent of the other two parts (U1, U2) which deal with setting and clearing the MOR bit.

4.3 As to the first difference (U3), the board is of the opinion that, in contrast to the decision, U3 is not entirely disclosed by D3. The passages cited in the decision (page 6, upper half of the page) as disclosure of U3, relate to different situations: paragraph [42] relates to scrubbing during *shutdown* (figure 3; [38]-[44]), while paragraph [46] relates to scrubbing during *booting* (figure 4; [45]-[56]). Accordingly, they cannot be combined to establish disclosure of U3.

4.4 However, the board considers that D3 discloses that a monitor program 202 (and not the BIOS as in the invention) scrubs the memory after trapping a shutdown request ([42], [43]; in the context of a process referred to as "dismantling the SE environment", which can be compared with disabling OS security in the invention). The board does not see which technical effect could be achieved by transferring the task of scrubbing from the monitor program (i.e. a program running below the OS-level) to the BIOS program (which also runs below the OS-level). The monitor program runs

in the processor's protection ring "0P" ([33], last sentence; figure 2: "0P" at the left hand side of Monitor 202), and the BIOS often runs in SMM (System Management Mode) in computers with x86 processors. In this context, SMM is sometimes called ring "-2" (see https://en.wikipedia.org/wiki/Protection_ring#Miscellaneous). The board does not recognise a technical effect of choosing any particular mode for the BIOS to run in and carry out its tasks.

4.5 The appellant merely asserted in general terms that the technical effect of the invention as a whole was to make the MOR bit (and thus scrubbing) "more usable" and "more flexible". However, the board cannot see that the invention is "more usable" than D3. Furthermore, the board does not consider "flexibility" by itself to be a technical effect.

4.6 Therefore, the board considers it to be an obvious alternative to have the BIOS rather than the monitor program of D3 scrub the memory during shutdown, and to run the BIOS in any particular "SMM" instead of protection ring "0P".

4.7 With respect to U1 (OS sets an MOR bit, grounds page 10), the board is of the opinion that the flag being set or cleared according to D3 to indicate that the memory might contain secrets or not ([24], sentence 6) constitutes an MOR bit within the meaning of the claim. The flag of D3 is used to decide whether or not to scrub during *booting* ([46], sentence 5; [51], first sentence; [55], first sentence).

4.8 The appellant argued that the meaning of the MOR bit and the flag of D3 are different. The MOR bit indicated that the memory had to be scrubbed during booting,

whereas the flag of D3 indicated that the memory contained or might contain secrets ([40], first sentence).

4.9 The board cannot agree with this distinction. Firstly, also the MOR according to the standard is set to ensure the scrubbing of memory because it might contain secrets and so as to delete these secrets, if any. And secondly, as explained above, the board considers as an MOR bit within the meaning of the claim any bit which has the claimed operational effects. Further differences, which are entirely in the mind of the observer, are of no technical relevance. The board also reiterates that the invention redefines the meaning of the MOR bit in that it allows scrubbing at shutdown and setting/clearing the bit in situations not foreseen in the original MOR bit definition. The passages in D3 show that the operational behaviour of the invention as claimed and D3 coincide sufficiently to consider the flag of D3 to constitute an MOR bit within the meaning of the claims.

4.10 The appellant further argued that the "information content" of the MOR bit and the flag of D3 are different. The flag in D3 could assume three states ("no secrets", "might have secrets" and "has secrets"), in contrast to the MOR bit which could only assume two states.

4.11 The board considers this assertion to be unfounded because, firstly, the term "flag" generally refers to a bit that can only assume two states. Secondly, D3 discloses the setting and clearing of the flag ([24], sentence 6), which only makes sense with a bit.

4.12 It is accepted, however, that D3 does not disclose which program sets this flag; it might be the OS 208 or the secure OS 212 (figure 2: "Kernel 212"). In the invention, it is the OS, but again the board cannot recognise which technical effect might be caused by this choice.

4.13 With respect to U2 (OS clears the MOR bit if a secret is deleted or if OS security is disabled), the board is of the opinion that D3 discloses clearing the flag if a secret is deleted in [43], sentence 4:

> "After erasing the system memory 108, the computing device 100 may update the secrets store 134 in block 312 to indicate that the system memory 108 does not contain secrets."

4.14 In the board's view, "updating the secrets store" includes updating the flag in the secrets store, i.e. clearing the flag after erasing (scrubbing) the memory.

4.15 The board considers that the second condition of U2 (OS clears the MOR bit ... if OS security is disabled) is obvious over the disclosure in D3, [50], first sentence:

> "... the flags of the secrets store 134 ... are initially cleared and are only set in response to establishing the SE environment 200."

4.16 It would be obvious for the skilled person to conclude from this that the flag can be cleared after the SE environment has been (successfully) dismantled (i.e. the OS security is disabled), because if OS security can be dispensed with, then the flag in the secrets store has no relevance for system security anymore.

Moreover, it is disclosed in D3 that the memory and its secrets are cleared in the process of dismantling the SE environment, since it is also disclosed ([24], sentence 6) that:

> "... the secrets store 134 may comprise a flag that may be set to indicate that the system memory 108 might contain secrets, and that may be cleared to indicate that the system memory 108 does not contain secrets."

It follows that after the dismantling process - i.e. once OS security is disabled - the memory is free of secrets so that the flag should be cleared.

4.17 The statement of grounds of appeal (page 14, paragraph 2) argues that the objective problem solved by the invention was to accelerate a subsequent booting process, with a reset attack still being prevented. Further (paragraph 3), D3 did not explicitly address the redundancy of memory scrubbing if the secret has already been deleted.

4.18 The board is of the opinion that this is not correct. D3, [43], sentence 5 discloses:

> "... the monitor 202 tracks with the secrets store 134 whether the system memory 108 contains secrets and erases the system memory 108 only if the system memory 108 contains secrets."

4.19 Thus, the subject-matter of claim 1 of the main request is not inventive.

5. As to the auxiliary requests, claim 1 of these requests differ from claim 1 of the main request in that it is the BIOS which clears the MOR bit, and not the OS as in feature U2 of the main request. However, the board cannot see which technical effect is achieved by having the BIOS rather than the OS clear the MOR bit.

5.1 These claims differ further from claim 1 of the main request in that the clearing is executed in SMM and during shutdown.

5.2 Similar to the main request, the board considers the execution in SMM to be an obvious choice.

5.3 Clearing the MOR bit during shutdown is disclosed in D3, [43], sentence 4 ("After erasing the system memory ..."; see above) which is performed during dismantling the SE environment during shutdown (see [42]), as explained above.

6. Claim 1 of auxiliary request 1 differs further from claim 1 of the main request in omitting the conditions (if a secret is deleted or OS security is disabled) for clearing. This obviously cannot establish an inventive step.

6.1 Thus, the subject-matter of claim 1 of auxiliary request 1 is not inventive either.

7. Claim 1 of auxiliary request 2 differs further from claim 1 of the main request and auxiliary request 1 in that the condition for clearing the MOR bit reads now:

> "in response to a secret being deleted from the confidential area (110) of the system memory (108) *while* OS security is enabled." (emphasis added)

7.1 The appellant intended this language to underline an alleged difference to D3. In D3 the MOR bit was cleared during the process of dismantling the SE environment (i.e. in the board's interpretation, when OS security is being disabled), while the MOR bit according to the invention may be cleared even if (and while) OS security remains enabled.

7.2 In the board's view, this does not establish an inventive step. According to D3, the SE is dismantled only after the flag is cleared ([43], sentences 1 and 4). If one takes the - in the board's view, reasonable - view that the "OS security" is disabled in D3 only once the SE environment is finally dismantled, one has to conclude that the MOR bit is cleared while OS security is still enabled. The board also notes that this corresponds well with the claim language: Although the MOR bit is claimed to be cleared "while OS security is enabled", it is also claimed to happen "during the shutdown process" (an option also disclosed in D3, [42]). The claim language does not imply that "OS security" might remain enabled after shutdown and the description lacks detail to explain what that might mean (see above, section 1.4). The board therefore cannot see that the added language establishes a clear difference over D3.

7.3 Thus, the subject-matter of claim 1 of auxiliary request 2 is not inventive either, and none of the requests fulfils the requirements of inventive step, in violation of Article 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

G. Nachtigall Martin Müller

Decision electronically authenticated