Internal distribution code:

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

Datasheet for the decision of 20 September 2018

Case Number: T 2324/12 - 3.5.06

Application Number: 07839061.4

Publication Number: 2069994

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
PERSISTENT SECURITY SYSTEM AND METHOD

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

Headword:
Persistent Security/HEWLETT-PACKARD DEVELOPMENT CO.

Relevant legal provisions:
EPC 1973 Art. 84, 83, 56

Keyword:
Claims - clarity (yes)
Sufficiency of disclosure - (yes)
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 2324/12 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 20 September 2018

Appellant: (Applicant)	Hewlett-Packard Development Company, L.P. 11445 Compaq Center Drive West Houston, TX 77070 (US)
Representative:	Zimmermann, Tankred Klaus Schoppe, Zimmermann, Stöckeler Zinkler, Schenk & Partner mbB Patentanwälte Radlkoferstrasse 2 81373 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 25 June 2012 refusing European patent application No. 07839061.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	A. Teale
	S. Krischer

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 25 June 2012, to refuse European patent application No. 07 839 061.4 on the basis that, in view of the expression "the HDD (44) comprising an encrypted HDD", claims 1 and 2 were unclear, Article 84 EPC. In a section entitled "Remarks", the examining division stated that executing a routine on an encrypted HDD would not have been a matter of common general knowledge for the skilled person, so that the invention was insufficiently disclosed, Article 83 EPC.

II. A notice of appeal and the appeal fee were received on 8 August 2012. The appellant requested that the decision be set aside and a patent granted.

III. With a statement of grounds of appeal, received on 23 October 2012, the appellant filed amended claims according to a new sole request. The appellant requested that the decision be set aside and that a patent be granted on the basis of the new sole request and the remaining application documents on file.

IV. In an annex to a summons to oral proceedings the board set out its provisional opinion that the amended claims overcame the clarity objection, Article 84 EPC 1973, upon which the decision was based. The appellant had also provided arguments overcoming the doubts raised in the decision regarding added subject-matter. However, although lack of inventive step had not been a reason for the appealed decision, an objection of lack of inventive step had been raised in the WOISA (Written Opinion of the International Searching Authority), based on D1 combined with either D4 or D5, and in the

communication of 4 November 2010 by the examining division, based on D2 in combination with D5, the cited documents being as follows:

D1: WO 98/43151 A1
D2: WO 2005/096122 A1
D4: US 6 510 512 B1
D5: US 6 148 387 A.

V. In a letter received on 17 August 2018 the appellant repeated the request that the decision be set aside and a patent granted on the basis of the following documents:

Description:
page 1, received on 2 March 2011,
page 1a, received on 30 March 2012 and
pages 2 to 7, as originally filed.

Claims:
1 and 2, received with the grounds of appeal.

Drawings:
Pages 1/2 and 2/2, as originally filed.

The appellant also provided arguments in support of inventive step, but did not submit any amendments.

VI. In a further submission, received on 12 September 2018, the appellant stated that neither the applicant nor its representative would attend the oral proceedings. The oral proceedings were then cancelled.

VII. The application documents on file are those set out above in point V, claim 1 reading as follows:

"A computing system (12), comprising: an operating system (OS)(34); a basic input/output system (BIOS) (24) having a boot routine (30) and a security routine (32); and a hard disk drive (HDD)(44) comprising a disk memory (56) for storing data in an encrypted format, wherein the computing system (12) is configured to: initiate (200) by the BIOS (24) a boot sequence of the computing system (12) using the boot routine (30), wherein a security authentication operation for obtaining and/or generating an encryption/decryption key (62) has not yet been performed by the OS (34) so that the HDD (44) is inaccessible by BIOS (24) during execution of the boot routine (30); transfer (202) control of the computing system (12) to the OS (34), when the BIOS (24) completed its share of the booting process of the computing system (12); initiate (204) by the OS (34) an encryption/decryption security routine (60) on the HDD (44), the encryption/decryption security routine (60) being stored in a master boot record sector of the disk memory (56) for encrypting data that is to be written to disk memory (56) and decrypting data retrieved from disk memory (56); retrieve and/or otherwise obtain (208) by the OS (34) an encryption/decryption key (62) associated with the HDD (44) for encrypting data to be stored on the HDD (44) and decrypting data retrieved from the HDD (44), when the security credential has been authenticated and/or otherwise validated (206); initiate (210) by the OS (34) a call to the BIOS (24); execute (211) by the BIOS (24) at least a portion of the security routine (32) to determine whether an instance (64) of the security routine (32) is present on the disk memory (56) of the HDD (44); if an instance (64) of the security routine (32) is present on the disk memory (56) of the HDD (44), return (218) control of the computing system (12) to the OS (34); if an instance

(64) of the security routine (32) is not present on the disk memory (56) of the HDD (44), retrieve (214) by the BIOS (24) an instance of the security routine (32), facilitate (216) by the BIOS (24) an instance of the security routine (32) to be stored on the disk memory (56) of the HDD (44) in an encrypted format via the encryption/decryption security routine (60), and return (218) control of the computing system (12) to the OS (34); and execute (220) by the OS (34) the instance (64) of the security routine (32) stored on the disk memory (56) of the HDD (44)."

Claim 2 sets out a corresponding method for providing an instance of a security routine on a hard disk drive of a computing system.

Reasons for the Decision

1. The admissibility of the appeal

In view of the facts set out at points I to III above, the appeal fulfills the admissibility criteria under the EPC and is consequently admissible.

2. Summary of the invention

2.1 The invention relates to a computer system comprising an encrypted hard disk drive (HDD). As shown in figures 1 and 2, when the system is booted the BIOS and then the operating system (OS) run initializing routines including those required to gain access to the encrypted hard disk (44)(steps 200 to 208). The BIOS (24) (basic input/output system) then checks to see if a copy of a security routine (64) is present on the hard disk. If none is present then the BIOS loads a copy of the routine from the embedded firmware (16, 32)

on the motherboard (20) to the HDD (44, 64)(steps 210 to 218). The OS then executes the security routine on the HDD (step 220); see paragraph [6].

2.2 According to paragraph [8], the security routine implements asset protection by contacting a remote security service (36) via a communication network (38) to determine whether the computer system has been reported as lost or stolen and, if so, causing the OS to log an Internet protocol IP or to facilitate tracking of the computer.

2.3 The HDD (44) comprises a processor (54) and disk memory (56), data being stored to disk memory in an encrypted format. According to paragraph [10], second sentence, "HDD 44 comprises an encrypted HDD 44 such that data stored to disk memory 56 is stored in an encrypted format". An encryption/decryption security routine (60) is stored in a master boot record sector of the disk memory (56) for encrypting data being written to memory and decrypting data being read from memory; see paragraph [10].

3. The prior art

3.1 Common general knowledge

3.1.1 In examination proceedings an inventive step objection was raised based on common general knowledge. The claimed invention was directed to a common secure computing system comprising an OS, a BIOS and an encrypted HDD in which the BIOS writes an instance of a security routine to the HDD if an instance of the security routine is absent from the HDD. It would however have been usual in such a system that the OS initiated a call to the BIOS when it needed to write to

the HDD, for instance when writing an instance of a security routine such as a security-related update or an anti-virus program to the HDD. The subject-matter of claim 1 was consequently not inventive.

3.2 Document D1

3.2.1 D1 relates to a system for locating and monitoring electronic devices using a security system (termed an "agent") embedded within the software, firmware or hardware of a computer. The security system causes the computer to periodically call a host system to provide unique identifying indicia and location information. According to figures 7A; 753 and 7B; 757, device tracking is performed by the BIOS component of the agent. According to page 39, lines 17 to 25, and figure 6C an image of the agent is transferred to the hard-disk of the computer (step 735) if none is already there. The image on the hard-disk is then loaded into memory and run.

3.2.2 The Written Opinion of the EPO as International Searching Authority (WOISA) raises an inventive step objection starting from D1 and combining it with either D4 or D5. The subject-matter of claim 1 differed from the disclosure of D1 in that the OS was configured to initiate a call to the BIOS to cause the BIOS to write an instance of a security routine to the HDD, instead of the BIOS performing this task autonomously. The problem solved by the invention was therefore "how to instruct the BIOS to refresh the agent image when the system is operational".

3.2.3 It would have been a usual design choice for the person skilled in the art to have the operating system trigger the execution of the BIOS routine (see, for example, D4

column 2, lines 41 to 44, or D5 column 2 lines 17-19 and column 9 lines 14-48).

3.3 Document D2

3.3.1 D2 relates to a communications driver agent (CDA) stored in hardware, firmware or software in an electronic device, such as a laptop (see page 12, lines 25 to 29), the CDA causing the electronic device to contact a monitoring server so that the electronic device can be tracked; see abstract. Page 3, lines 4 to 6 and 28 to 30, mentions tracking software being removed from stolen corporate computers which are then used to attack the corporate computer network. According to page 21, line 22, to page 22, line 5, a CDA is installed from ROM on to the hard-disk and runs as a service of the operating system.

3.3.2 In the communication dated 4 November 2010 the examining division raised an inventive step objection starting from D2. The subject-matter of claim 1 differed from the disclosure of D2 in that, instead of the BIOS, the OS was configured to initiate the call to the BIOS. The technical effect of this difference was that the persistence of the security routine was improved in the case of systems which were not regularly booted. The problem solved by the invention was "how to improve the persistence of the security routine in the case of systems which are not regularly booted". When implementing the system of D2, the skilled person would have considered the passages (see page 3, lines 4 to 6, and page 3, lines 28 to 30) concerning the threat arising from a stolen computer, whose tracking software has been removed, being used to penetrate a corporate network using the preconfigured network access. The skilled person would have been

aware that corporate networks often have many assets with network access which are not rebooted regularly or at all (e.g. NAS and computers going into "hibernation" mode instead of being switched off). Hence the skilled person would have realised that a thief would seek to remove or disable the full-function CDA of D2 without rebooting. Thus the skilled person would have been prompted to re-trigger the installation of the security routine while the OS was running.

3.3.3 One standard method of re-triggering would have been for the OS to call the BIOS function, as known, for example, from D5; see column 2, lines 17 to 19 and column 9, lines 14 to 48. By applying the teaching of D5 to the apparatus of D2, the skilled person would have arrived at the subject-matter of claim 1 in an obvious manner.

3.4 Document D4

D4 relates to a computer system comprising a BIOS file on a hard-disk, BIOS code within the BIOS file being copied to an executable program file and executed by a processor. According to column 2, lines 41 to 44, D4 is aimed at enabling an operating system to emulate BIOS routines.

3.5 Document D5

According to its abstract, D5 relates to the secure use of BIOS services in a computer in which service requests to the BIOS contain a signature generated using a private key of a cryptographic key pair.

4. The appealed decision

4.1 According to the reasons for the decision (section II), the expression "the HDD (44) comprising an encrypted HDD" in claims 1 and 2 was unclear, Article 84 EPC, since it contained a recursive definition, a similar expression being used in the description; see paragraph [10].

4.2 In a further section III, entitled "Remarks", the examining division expressed doubts as to sufficiency of disclosure, Article 83 EPC. The initiation of the encryption/decryption security routine on the HDD and the HDD comprising an encrypted HDD, both features being set out in claim 1, when considered together, gave rise to doubts as to where the "encryption/ decryption security routine" was stored and whether it was stored in an encrypted form or not. In the embodiment shown in figure 1 and described in paragraph [10] the routine was stored in encrypted disk memory, i.e. it was stored on an encrypted HDD in an encrypted format. Putting the invention into practice would thus have required the execution of a routine on an encrypted HDD, which was not a matter of common general knowledge for the skilled person and was not explained in the application.

5. The grounds of appeal

5.1 The appellant has argued that the amendments to the claims overcome the clarity objection (see point 1 of the decision) upon which the decision was based and also make clear that the security routine was stored in the disk memory of the HDD in encrypted form.

5.2 In response to the doubts raised regarding sufficiency of disclosure (point 2 of the decision), the appellant has pointed out that both the description (paragraph [10]) and claim 1 set out the encryption/decryption security routine being stored in a master boot record sector of the disk memory (56). The skilled person would have understood from this that the routine was provided in an unencrypted format.

6. The board's understanding of how the invention works

6.1 In view of figure 1, HDD 44 only stores the asset protection security routine (if present) and the encryption/decryption security routine. The OS (34), for instance, is stored elsewhere and can be accessed without an encryption key or decryption. The encryption/decryption security routine is stored in a master boot record sector of the disk memory (56); see paragraph [10]. The skilled person would have been aware that the master boot record sector of a disk memory does not contain data, in the sense of the data to be stored in and recalled from the disk. Instead it contains information on the logical disk partitions and executable code for accessing the disk. In the light of the application as a whole, the encryption/decryption security routine cannot be encrypted, since there is no other functionality for decrypting it. Hence the board understands that, although data is stored in the disk memory (56) of the HDD (44) in encrypted form, the encryption/decryption security routine (60) itself is stored in the disk memory in unencrypted form. To do its work, the encryption/decryption security routine requires a key, which can be obtained (step 208) from the trusted platform module (TPM) (18) on the motherboard (20); see paragraph [1], last sentence.

6.2 After the system has booted, it ensures that a copy of the asset protection security routine (64) is stored in the disk memory (56) in encrypted form, the BIOS if necessary reloading a copy from firmware (32) if the routine is not present. The routine is then run by the OS. The board understands that, in order to run the asset protection security routine, it is first decrypted by the HDD processor (54) and transferred to the main memory (not shown in the figures) of the computing system where it is executed.

7. Clarity, Article 84 EPC 1973

7.1 The board understands the expression in paragraph [10] of the description "HDD 44 comprises an encrypted HDD 44 such that data stored to disk memory 56 is stored in encrypted format" in the sense of the previous sentence in the description, namely that "... HDD 44 comprises a processor 54 and disk memory 56", i.e. that the second use of HDD 44 should be understood as "disk memory 56".

7.2 The expression objected to in the decision has now indeed been amended to read "a hard disk drive (HDD) (44) comprising a disk memory (56) for storing data in an encrypted format" and thus overcomes the clarity objection in the decision.

8. Sufficiency of disclosure, Article 83 EPC 1973

8.1 According to the board's understanding of the invention, set out above, the asset protection security routine is first decrypted by the HDD processor (54) and transferred to the main memory of the computing system where it is executed. Hence putting the invention into practice would not, as the "Remarks" section of the decision asserts, have required the

skilled person to execute the routine while still encrypted on the HDD.

8.2 The board is thus satisfied that the invention is sufficiently disclosed, Article 83 EPC 1973.

9. Inventive step, Article 56 EPC 1973

9.1 Although lack of inventive step was not a reason for the decision, such objections were raised in the WOISA, based on D1 combined with either D4 or D5, and in the communication by the examining division of 4 November 2010, based on D2 in combination with D5.

9.2 According to page 1a of the description, the invention seeks to solve the problem of "handling service routines using an encrypted hard disk". Both D1 (see page 39, lines 23 to 25) and D2 (page 12, lines 25 to 29), summarized above, relate to storing tamper-resistent security (tracking) routines on the hard disk of computers.

9.3 It is common ground between the board and the appellant that the subject-matter of claim 1 differs from the disclosure of either D1 or D2, taken separately, in that:

a. the encryption/decryption security routine is stored in a master boot sector record sector of the disk memory, and

b. the OS is configured to initiate calls to the BIOS to check for the presence of and, if necessary, to write an instance of the security routine to the HDD.

It is also common ground that neither of documents D4 or D5 discloses either feature "a" or "b". The board takes the view, which the appellant has not challenged, that these difference features are unrelated, so that their contributions to inventive step must be considered separately.

9.4 Regarding difference "a", the skilled person would have been aware that it is usual to store executable code for accessing a hard disk in the master boot sector record sector. Hence the board regards this feature as a matter of usual practice for the skilled person, the appellant not having disputed this view.

9.5 Regarding feature "b", the appellant has pointed to what it sees as a "contradiction" in the annex to the summons between the summary of the examining division's assessment in point 6.3.2 and the board's assessment in point 9.4.2. The examining division took the view that feature "b" had the technical effect of improving the persistence of the security routine in the case of systems which were not regularly rebooted. The board however is not persuaded that feature "b" has a technical effect, in particular because the claim does not set out a further technical effect of the security routine. The appellant has also argued that, by using the OS to initiate checking for the presence of a security routine, security is improved in devices that are rarely rebooted. This argument presupposes that the BIOS only plays a part during the booting of a computer. However the skilled person would be aware that an OS can make calls to BIOS functions after booting. Moreover the partitioning of functions between a BIOS and an OS would have been a matter of usual design for the person skilled in the art of computer design. Hence the board finds that feature "b" has no

further technical effect and thus cannot contribute to inventive step.

9.6 Consequently the board finds that the subject-matter of claim 1 does not involve an inventive step, Article 56 EPC 1973, starting from either D1 or D2, taken separately.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated