Internal distribution code:

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

Datasheet for the decision of 4 September 2018

Case Number: T 1959/12 - 3.5.06

Application Number: 09729198.3

Publication Number: 2277128

IPC: G06F21/24

Language of the proceedings: EN

Title of invention:
AN ANTI-TAMPER SYSTEM EMPLOYING AUTOMATED ANALYSIS

Applicant:
INSIDE SECURE

Headword:
Software anti-tamper measures/INSIDE SECURE

Relevant legal provisions:
EPC Art. 84

Keyword:
Claims - clarity (no) - support in the description (no)

Decisions cited:
T 0296/93

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 1959/12 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 4 September 2018

Appellant: (Applicant)	INSIDE SECURE Rue de la Carrière de Bachasson, CS 70025 Arteparc Bachasson, Bât. A 13590 Meyreuil (FR)
Representative:	de Jong, Jean Jacques Omnipat 24, place des Martyrs de la Résistance 13100 Aix en Provence (FR)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 30 March 2012 refusing European patent application No. 09729198.3 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 30 March 2012 to refuse European patent application No. 09 729 198.3 *inter alia* on the basis that the subject-matter of claim 1 lacked inventive step, Article 56 EPC, in view of the document

D1: US 2007/0256138 A1

and well-established techniques in the field of software protection, as exemplified by

D2: US 6 668 325 B1.

II. A notice of appeal was received on 7 June 2012, the appeal fee being paid the next day. The appellant requested that the decision be set aside, that the application be granted. The appellant also requested that the appeal fee be reimbursed, but later did not maintain this request at the oral proceedings.

III. In a statement of grounds of appeal, received on 7 August 2012, the appellant requested that the subject-matter of all claims be found to be patentable, that the decision be set aside and that the case be remitted to the first instance for grant. An auxiliary request was made for oral proceedings.

IV. In an annex to a summons to oral proceedings the board set out its provisional opinion that *inter alia* the application did not comply with Article 84 EPC regarding clarity. The board also had doubts whether the claimed subject-matter produced a technical effect going beyond the usual effects of program execution so

that the claimed subject-matter did not involve an inventive step, Article 56 EPC.

V. With a submission received on 26 June 2018 the appellant submitted new amended claims. The appellant requested that the subject-matter of the claims be found to be patentable and that the oral proceedings be held in French.

VI. In a communication dated 6 July 2018, sent via its registry, the board stated that the appellant's arguments and amendments seemed to overcome the board's objections *inter alia* under Article 84 EPC. The board however still had doubts regarding inventive step, Article 56 EPC, since the claims did not set out, nor did the application as filed disclose, an enforcement step, i.e. a technical consequence (such as terminating the program) automatically triggered if the integrity checks detected tampering. Concerning the appellant's request to hold the oral proceedings in French, the appellant, having made a request in due time, Rule 4(1) EPC, was now entitled to use French as well as English at the oral proceedings. In view of Rule 4(4) EPC, the appellant should however be prepared for the board to use the language of the proceedings (English) as well as French at the oral proceedings. Regarding the request for reimbursement, Rule 103(1)(a) EPC, the board pointed out that the appellant had not provided any arguments as to why a possible substantial procedural violation had occurred before the first instance.

VII. In a response, received on 19 July 2018, the appellant proposed three possible options for amendments to claim 1 aimed at overcoming the objection of lack of inventive step by setting out an enforcement step. The

appellant requested that the oral proceedings be cancelled and that the proceedings be continued in writing.

VIII. In a communication dated 26 July 2018, sent via its registry, the board stated that the oral proceedings would take place as scheduled.

IX. With a submission, received the day before the oral proceedings on 3 September 2018, the appellant submitted a new set of amended claims.

X. At the oral proceedings, held on 4 September 2018 in English and French, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims filed on 3 September 2018.

XI. At the end of the oral proceedings the chairman declared the debate closed. After deliberation, the board then announced its decision.

XII. On 5 September 2018, the day after the oral proceedings, a submission dated the same day was received from the appellant containing further arguments and a request to continue the appeal proceedings in writing.

XIII. The application is being considered in the following form:

Description: pages 1 to 20, received on 26 September 2011.

Claims: 1 to 25, received 3 September 2018.

Drawings: page 1/1, as originally filed.

XIV. Claim 1 reads as follows (emphasis added by the board):

"A computer implemented anti-tamper system operable to:

(i) profile at runtime an executable application software to provide profile information about the application software,
(ii) determine injection positions where to inject integrity checks into a source code of the application software, using the profile information, the profile information identifying functions in the application software where to inject the integrity checks, each of the integrity checks enabling a subsequent verification of whether or not the application software has been tampered with, a **defensive action** being taken when one of the integrity checks detects a modification of the application software,
(iii) inject the integrity checks into the source code at the determined injection positions, which produces a modified source code, and
(iv) generate a protected executable application software from the modified source code,
characterised in that the profile information comprises frequency-domain information recording frequencies at which each function of the application software is called, and during which time range each frequency occurs, the determination of the injection positions comprising:
selecting an injection position in a lower-frequency function to reduce performance overhead of the application software;
selecting an injection position in a higher-frequency function to increase a protection level of the application software; and

detecting unstable functions based on the frequencies and time ranges recorded for each function and rejecting an injection position in an unstable function."

The claims also include an independent claim 21 to a method and claims 23 and 24 to a computer program.

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 satisfies the admissibility criteria under the EPC and is therefore admissible.

2. The appellant's submission received the day after the oral proceedings

This submission was received after the closure of the debate and the announcement of the decision. The board has not taken the content of this submission into account in the reasons for this decision, since, once a decision has been announced, the board is no longer empowered or competent to take any further action apart from issuing the written decision (see **T 296/93**, OJ 1995, 627, where the board disregarded statements filed after the announcement of the decision; see XIV and reasons 1.)

3. The admittance of the claims filed the day before the oral proceedings into the procedure

3.1 In the letter of 3 September 2018, the day before the oral proceedings, accompanying the amended claims the

appellant explained that the amendments corresponded to "option 3", proposed by the appellant in the earlier letter of 19 July 2018.

3.2 According to Article 13(1) RPBA, any amendment to a party's case after it has filed its grounds of appeal or reply may be admitted and considered at the board's discretion. The discretion shall be exercised in view of *inter alia* the complexity of the new subject-matter submitted, the current state of the proceedings and the need for procedural economy. Under Article 13(3) RPBA amendments sought to be made after oral proceedings have been arranged shall not be admitted if they raise issues which the board or the other party or parties cannot reasonably be expected to deal with without adjournment of the oral proceedings.

3.3 In the present case, the board is satisfied that the amendments are directed to overcoming the objection under Article 56 EPC raised by the board in the annex to the summons to oral proceedings, the limited extent of the amendments, which had also been mentioned over a month before the oral proceedings, being such that the board was readily able to assess their effect. Hence the board admitted the new set of claims into the procedure.

4. Summary of the invention

4.1 The invention relates to modifying the source code of application software, for instance gaming software (see the paragraph bridging pages 2 and 3), to enable the integrity of the software to be checked when it is run; see page 16, line 21, to page 17, line 13. The aim is to prevent hackers from modifying the software to change its behaviour; see page 1, lines 23 to 26. For

instance, hackers may seek to remove "trial" limitations and distribute "hacked" versions of the software. "Anti-tamper" systems seek to prevent this; see page 1, lines 28 to 33. According to page 2, lines 26 to 28, if modifications to the application code are detected then "defensive action can be taken".

4.2 The approach used by the invention involves runtime **profiling** the software to identify one or more functions, **deciding** where to inject integrity checks into the source code to enable verification of whether or not the software has been tampered with and **injecting** integrity checks into the or each function in the source code, as established by the runtime profiling.

4.3 **Profiling** involves a "pre-instrumentation" step involving an initial static analysis of the application to enumerate its functions. Runtime profiling is then carried out by making instrumenting modifications to the application source code and compiling it. Data is then collected by running the instrumented application to provide at least some of layout, structure and timing information about the application; see page 11, lines 24 to 27, and page 12, lines 1 to 5. For example, the following data is collected: function execution counts, execution times and frequency-domain data on the frequencies at which any given function is called; see page 12, lines 7 to 33.

4.4 In **deciding** where to inject integrity checks (termed the "injection policy" on page 17, lines 28 to 29) into the source code, there is a trade-off between impacting performance and maximising protection against tampering; see page 17, lines 18 to 22. Functions are also avoided as injection targets which execute at a

large number of different frequencies during profiling (termed "temporally unstable").

4.5 **Injecting** integrity checks into the source code involves inserting code and compiling it to give the "protected application"; see page 11, lines 27 to 29.

5. Clarity and support, Article 84 EPC

5.1 Claim 1 now sets out the consequence of detecting tampering as "**defensive action** being taken when one of the integrity checks detects a modification of the application software" (emphasis added by the board).

5.2 In the oral proceedings the Board raised objections under Article 84 EPC questioning clarity and support of the aforementioned newly introduced feature. The appellant argued that the skilled person would understand from the application that "defensive action" referred to actions which were appropriate for improving the protection of the software. Such actions could however not rely on the Internet, since the application might be running on a computer isolated from the Internet. An appropriate defensive action would, for example, be to terminate the application.

5.3 The board finds that the application provides no explanation of the expression "defensive action" or examples of it. The appellant has also provided no evidence that the term "defensive action" has an accepted meaning in the art and would thus be familiar to the skilled person. The board is also unaware of a generally accepted meaning of the expression. The term "defensive action" might, for example, be understood to cover displaying a warning that the software had been modified contrary to its licence conditions or instead

to cover, at the next opportunity, sending information via the Internet identifying the application and the user to a server operated by the software vendor. Either action could be seen as an appropriate alternative to terminating the program. Under these circumstances the board takes the view that the technical meaning of the expression "defensive action" is unclear. It is also unclear where the limits of "defensive action" lie, for example whether it excludes actions using the Internet or not.

5.4 Hence claim 1 is unclear and not supported by the description, contrary to Article 84 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated