Internal distribution code:

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

Datasheet for the decision of 11 October 2022

Case Number:	T 2562/17 - 3.5.06
Application Number:	09725211.8
Publication Number:	2256661
IPC:	G06F21/00, G06F21/24, G06F21/06
Language of the proceedings:	EN

Title of invention:
ELECTRONIC TERMINAL, CONTROL METHOD, COMPUTER PROGRAM, AND INTEGRATED CIRCUIT

Applicant:
Panasonic Intellectual Property Management Co., Ltd.

Headword:
Electronic terminal/PANASONIC

Relevant legal provisions:
EPC Art. 56
EPC R. 103(4)(c)

Keyword:
Inventive step - (no)

This datasheet is not part of the Decisior
It can be changed at any time and without notic

Decisions cited:

Catchword:

This datasheet is not part of the Decisior
It can be changed at any time and without notic

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 2562/17 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 11 October 2022

Appellant: (Applicant)	Panasonic Intellectual Property Management Co., Ltd. 7 OBP Panasonic Tower, 1-61, Shiromi 2-chome, Chuo-ku, Osaka-shi, Osaka 540-6207 (JP)
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 11 May 2017 refusing European patent application No. 09725211.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	A. Teale
	A. Jimenez

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 11 May 2017, to refuse European patent application No. 09 725 211.8 on the basis that the subject-matter of the claims lacked inventive step, Article 56 EPC, either in view of notorious prior art or a document referred to as D1.

II. A notice of appeal and the appeal fee were received on 13 July 2017, the appellant requesting that the decision be set aside and a patent granted. The appellant also made an auxiliary request for oral proceedings.

III. In a statement of grounds of appeal, received on 12 September 2017, the appellant requested that the decision be set aside and a patent granted on the basis of the claims of 25 March 2014 (main request) or those of 14 February 2017 (auxiliary request), the description being that in the decision. The appellant also refiled the claims of the main and auxiliary requests and reiterated the auxiliary request for oral proceedings.

IV. In an annex to a summons to oral proceedings the board set out its provisional opinion on the appeal that *inter alia* it tended to agree with the negative conclusion on inventive step regarding both requests reached in the decision.

V. In a letter received on 5 October 2022 the appellant withdrew the request for oral proceedings and requested that a decision be issued in writing. The appellant further requested a 25% reimbursement of the appeal fee. No substantive arguments were made or amendments submitted. The board subsequently cancelled the oral proceedings.

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

Description (both requests):
pages 2 to 60, as published, and pages 1 and 1a, received on 30 January 2013.

Claims (all refiled with the grounds of appeal):
Main request: 1 to 13, received on 25 March 2014.
Auxiliary request: 1 to 12, received on
14 February 2017.

Drawings (both requests):
Pages 1/20 to 20/20, as published.

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

"An electronic terminal comprising: a first storage unit (216) for storing therein confidential information to be protected; a plurality of protection measures that constitute a security implementation model, and are operable to intercept an access from the external source to the confidential information; a plurality of monitoring units (211, ...211n) operable to monitor for an attack to any of the plurality of protection measures from the external source a second storage unit (204) for storing therein (i) value information that is attached to the confidential information and expresses a value of the confidential information, and (ii) a plurality of defense level information pieces each attached to one of the plurality of protection measures and expressing a defense level value of a corresponding protection measure against an attack from the external source, the value of the confidential information being an indicative value calculated based on an amount of loss anticipated if the confidential information is stolen, and the defense level value expressed by a given defense level information piece being an indicative value calculated based on a cost for analysis of the corresponding protection measure and applied [on] the same scale as the value of the confidential information; and a control unit (207) operable to, when (i) an attack to any of the plurality of protection measures has been detected, and (ii) a sum of defense level values for protection measures that have not been attacked remaining in the security implementation model is less than the value expressed by the value information that is attached to the confidential information, update a protection measure that can be updated among the remaining protection measures in the security implementation model so that after the update, the protection measure that can be updated has a higher defense level compared to before the update and so that the sum of the defense level values for the remaining protection measures in the security implementation model is greater than the value expressed by the value information that is attached to the confidential information."

VIII. Claim 1 of the auxiliary request differs from that of the main request in that it has been paraphrased to set out the same subject-matter.

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 requirements under the EPC and is consequently admissible.

2. The request for reimbursement of the appeal fee at 25%

2.1 According to Rule 103(4)(c) EPC, the appeal fee shall be reimbursed at 25% if any request for oral proceedings is withdrawn within one month of notification of the communication issued by the Board of Appeal in preparation for the oral proceedings, and no oral proceedings take place.

2.2 In this case the summons to oral proceedings was deemed notified (Rule 126(2) EPC) to the appellant 10 days after it was posted on 8 September 2022, that is on 18 September 2022. Hence the time limit for withdrawing the request for oral proceedings under Rule 103(4)(c) EPC expired on 18 October 2022 . As the withdrawal of the request for oral proceedings reached the EPO on 5 October 2018, which was before said expiry date, and the oral proceedings were subsequently cancelled by the board and therefore did not take place, the conditions for the reimbursement of the appeal fee at 25% are fulfilled.

3. Summary of the invention

3.1 The invention concerns detecting unauthorized analysis of an electronic terminal device and preventing unauthorized acquisition and falsification of confidential information. Essentially, if the terminal detects that attempts have been made to access confidential information, then the measures used to protect that information are intensified, thus protecting data confidentiality and integrity.

3.2 To do that, the terminal (102)(see figure 2) stores value information relating to confidential information. When an access attempt (attack) regarding a protection measure along an attack route between an external source and the confidential information is detected by one of several monitoring units, one of the protection measures, each having a defense level value, is "updated" so that the sum of the defense level values of the remaining (understood as "non-compromised") protection measures along the "partial route" is greater than or equal to the value information.

3.3 One protection measure is encryption; see [64] and figure 3; 232. Updating this protection measure involves updating the encryption program. The terminal comprises a key generation program for generating a decryption key [15], and attempts to access the key generation program via a "second attack route" are monitored. The terminal also comprises means for storing a program for accessing a decryption key. Defences against attack may be strengthened by updating the decryption program which may also be obfuscated (rendered obscure); see [20-22].

3.4 A further protection measure (see [50]) is to conceal or disable a "debugger terminal", used for authentication when connecting a debugger device to the terminal for carrying out operational tests on the terminal prior to shipping.

3.5 The result of the comparison of the sum of defence level values with the value information may be transmitted to a management server (see figure 1; 101, figures 5, 12 and 20, and figure 10; 1101) comprising a communication unit and a control unit (see [35]), which responds with a new protection measure; see [25]. This approach has the advantage that new protection measures need not be stored in the terminal where they could be the target of an attack; see [27].

3.6 The description and drawings disclose several embodiments of the invention. According to embodiment I (see [44] and figures 1 to 2), figure 1 shows a plurality of electronic terminals (102a, 102b) communicating via a network (103) with a server (101). A terminal is a computer system consisting of a CPU (Central Processing Unit), RAM (Random Access Memory), a drive device and a network connection device; see [48]. According to [49], the confidential information may include a device ID or key, an authentication code or program for authenticating messages between the terminal and the medium on which a computer program is stored and a program for providing services to a user. Figure 2 illustrates the functional elements of the terminal; see [56-59].

3.7 Figure 3 illustrates the case of preventing an attack on a property (250) having a "property value" of 10 by encrypting it (232). One attack ([66]) is a "brute force" attack on the encryption. The corresponding first attack path/protection path (260) has a total defense level of 20, consisting of the encryption step (10) and debugger concealment (10); see [115-120]. The other form of attack ([67]) is directed to the encryption key (251). The associated second attack path/protection path (261) has a defence level of 17, consisting of code obfuscation (2), debugger disabling (5) and debugger terminal concealment (10). The defence level of a particular protection measure is an estimate of the cost of overcoming (termed "analyzing") the measure, calculated as the product of three factors (see [72]): the cost of tools, the hourly wage of an engineer and the time required for analysis.

3.8 Each protection measure has an associated monitoring unit (211a-e) for detecting whether the protection measure has been attacked by an external source and, if so, notifying the detection information generation unit 201; see [78-80] and figure 2. An attack is detected by monitoring whether a device that should not be connected and is equipped with an analysis tool, such as a debugger, is connected to the terminal or whether a program implementing a protection measure has been illicitly rewritten, this being detected by comparing hash values; see [82]. The monitoring unit for debugger terminal concealment (231,241) monitors whether the concealed debugger terminal has performed authentication with an external source; see [81]. The monitoring units may monitor each other; see [83]. Each protection measure has an associated "protection identifier" (1-1 to 1-2 and 2-1 to 2-3), a history management table (see figure 4, T100) in a history management unit (205) storing *inter alia* the date and time of a detected attack on a protection measure; see [86-88].

3.9 Detection information from the history management table in the terminal is transmitted together with an update request by a transmission unit (214) (see [129-130]) to the server (101); see figure 5 and [139-165]. Detection information has an associated signature (see [98]) for certifying that it was generated by the terminal, thus demonstrating its authenticity; see [98-102]. The "detection information reception unit" 312 of the server verifies the authenticity of the detection information from the terminal using the terminal's public encryption key; see [143-146]. Authenticated detection information is passed to the "history management unit" (304) where it is stored together within a management ID identifying the terminal in a history management table (T200); see figure 6 and [147-150]. In response to the update request, the protection method selection unit 306 selects a protection method based on the one or more locations requiring an update and the defense levels required for each update location; see [156]. According to [163], the protection method selection unit 306 "replaces, that is to say updates," the model identifier corresponding to the management ID of the terminal with that of the acquired model information. The protection method delivery unit 310 (termed the "protection method transmission unit 310" in figure 5) transmits the new model information to the terminal.

3.10 The flow chart in figure 7 illustrates the actions of the terminal; see [167-174]. If a monitoring unit (211) detects (step S5) that a protection measure has been attacked by an external source then, if there is a network connection with the server (step S20), detection information is transmitted with a digital signature (step S25) to the server (step S30). If the terminal decides that an update is required, then the terminal receives new secure information from the server and updates the secure information in the terminal (step S35).

3.11 Figure 8 illustrates the update processing (step S35) in the terminal. The terminal determines whether an update is required by calculating (step S100) a defense level for each protection path including one or more protection measures that have been attacked. The "update requirement determination unit" 208 then compares the calculated defense levels with the value of the protected property (step S105); see [176-177]. If an update is found to be necessary, then the terminal determines one or more locations requiring an update and the defense level required at each location (step S110); see [178]. Based on this information, update request information is sent to the server (step S115, S120) which responds with secure information and one or more monitoring units (step 125). This information is then used by the terminal to update the information in secure storage (216) and the model information (230) in the current model storage unit (206); see [181].

3.12 The flowchart in figure 9 (see [183-190]) illustrates the corresponding server operations. The digital signature of detection information from terminals is verified (step S205) and the information stored (step S210). Requests for update information are received (step S215), new secure and model information and monitoring units are selected (step S220) and this information is transmitted to the terminals (step S225).

3.13 So far, the first embodiment of the invention has been described. Paragraphs [191-277] and figures 10 to 15 relate to the second embodiment. According to [191], the second embodiment differs from the first in that, when an attack is detected, the calculation of defense levels and the determination of update locations occurs in the server. Figures 16 to 20 and paragraphs [284-359] relate to a third embodiment in which the protection method can be upgraded for a version upgrade or, after the defense level of a protection measure has been reduced, understood to mean that the measure has been compromised, by successfully deciphering the encryption or deciphering a code that has been code obfuscated; see [285]. Paragraphs [360-414] relate to possible modifications of the first two embodiments, paragraphs [415-426] set out the hardware components used to construct a computer system according to the invention, and paragraphs [427-466] summarise the invention.

4. The board's understanding of the invention

4.1 The board understands the expression in original claim 1 and the description (see, for instance, [7]) "an attack route extending from an external source to the confidential information" not as a physical "path" such as a series of locked doors blocking access to a vault. The expression implies an ordered sequence of operations that would have to occur before the confidential information could be accessed. The fact that the defense levels are "summed" before being thresholded implies that the measures are complementary/cumulative, but no "sequence" is necessarily implied: a single door could be secured by several locks, or one locked door could lead to another; see the measures relating to be debugger, for instance.

4.2 The board finds that the computation and comparison of the "defense levels" and the "value" of the confidential information are non-technical. The three parameters used to calculate the security levels (the cost of tools, the hourly wage of an engineer and the time required for analysis) are not technical, and no criteria are disclosed for computing the value of confidential information.

4.3 In view of the foregoing, the board interprets claim 1 as setting out the protection of confidential information by a number of complementary protection measures with an associated "defense level" and, if the sum of all such levels of non-compromised protection measures falls below some predefined threshold, the non-compromised protection measures are improved, if possible. Claim 1 sets out comparing the "value" of the remaining protection with the value of what is protected to update a remaining (non-compromised) protection message. The invention does not involve updating the compromised protection measure.

4.4 All in all, the process according to the invention is regarded as a non-technical administrative scheme.

5. Clarity, Article 84 EPC

5.1 Despite the issues raised in the annex to the summons to oral proceedings, the board finds that claim 1 of both requests is sufficiently clear for the purposes of assessing inventive step.

6. The "notorious" prior art

6.1 In the case law of the boards of appeal, prior art that was so well known at the priority date that no documentary evidence need be provided to prove its existence is referred to as "notorious" prior art; see Case Law of the Boards of Appeal of the EPO, 9th edition, IV.B.4.1.3.

6.2 The decision refers (see points 3.5 and 3.6 of the reasons) to a "conventional electronic terminal with its standard data processing and storage capabilities" which was notoriously known before the priority date (25 March 2008) of the present application.

6.3 The board has no doubt that such computing devices with processing and storage capabilities were indeed "notorious" before the priority date.

7. Inventive step, Article 56 EPC

7.1 According to the appealed decision, the subject-matter of the independent claims lacked inventive step in view of two separate lines of argument based firstly on a notorious electronic terminal and secondly on the disclosure of D1.

7.2 In its preliminary opinion, the board addressed both lines of argument. This decision can, however, be limited to the first one, according to which the independent claims related to the technological implementation of an abstract threat mitigation model and to mathematical calculations within the model for a cost-benefit analysis. In view of the references in the claims to an "electronic terminal", the claimed subject-matter fulfilled Article 52(1) EPC regarding technical character. The claims set out a mixture of technical and non-technical features, the latter relating to the abstract threat mitigation model and to mathematical calculations within the model for a cost-benefit analysis which could legitimately appear in the formulation of the technical problem. Some of the non-abstract features of claim 1 had no technical effect, leaving the following non-abstract features having a technical effect: an electronic terminal comprising a storage unit and a storage measure. Based on these features, the closest prior art was a conventional electronic terminal with its standard data processing and storage capabilities, such terminals being notorious prior art at the priority date, no written evidence being required. As the non-abstract features were known from this prior art, claim 1 lacked inventive step.

7.3 In the grounds of appeal the appellant did not comment on the first line of argument.

7.4 As the board indicated in its provisional opinion and as stated above (point 6), the board agrees with the decision that the "notorious" prior art relied on in the first line of argument was indeed so commonly known in the art that no written evidence is required to establish it.

7.5 The board agrees with the result and the reasoning of the decision under appeal that the skilled person, starting from such a device and given an aim to be achieved in a non-technical field of implementing the administrative scheme consisting of the threat mitigation model and the mathematical calculations within the model for a cost-benefit analysis (see point

4 above), would have arrived at the subject-matter of claim 1 of both requests without an inventive step.

7.6 Hence the board finds that claim 1 of both requests does not involve an inventive step, Article 56 EPC.

Order

For these reasons it is decided that:

1. The appeal is dismissed.
2. The appeal fee is to be reimbursed at 25%.

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

M. Müller

Decision electronically authenticated