Internal distribution code:

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

Datasheet for the decision of 15 December 2017

Case Number: T 1073/15 - 3.5.06

Application Number: 12188083.5

Publication Number: 2696307

IPC: G06F21/34, G06F21/35, G06F21/40, G06F21/12, G06F21/62

Language of the proceedings: EN

Title of invention:
System and method for controlling user's access to protected resources using multi-level authentication

Applicant:
Kaspersky Lab, ZAO

Headword:
Multi-level authentication/KASPERSKY

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 1073/15 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 15 December 2017

Appellant: (Applicant)	Kaspersky Lab, ZAO 39A/3 Leningradskoe Shosse Moscow 125212 (RU)
Representative:	Sloboshanin, Sergej V. Füner, Ebbinghaus, Finck, Hano Mariahilfplatz 3 81541 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 15 January 2015 refusing European patent application No. 12188083.5 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	G. Zucka

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dispatched on 15 January 2015, to refuse European patent application No. 12 188 083.5, because independent claims 1 and 8 extended beyond the application as originally filed and lacked inventive step over

D1: EP 1 684 204 A1

as the obvious implementation of non-technical requirements.

II. Notice of appeal was filed on 9 March 2015, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 11 May 2015. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of claims 1-14 as filed with the grounds of appeal; description, pages 1, 2, 2a, 2b, 3 as filed on 18 June 2013; as well as pages 4 to 16 as originally filed; drawings; sheets 1/7 to 5/7 and 7/7 as originally filed; and sheet 6/7 as filed on 18 June 2013.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention lacked inventive step over D1, Article 56 EPC. Objections under Articles 84 and 123(2) EPC were also raised.

IV. In response to the summons, the appellant filed neither amendments nor arguments. With a letter dated 7 December 2017, it withdrew its request for oral proceedings, which were then cancelled.

V. Claim 1 of the sole request reads as follows:

"A method for controlling user's access to a protected resource, the method comprising:

detecting a plug-in token (111, 112) connected to a device (100, 200) that controls user access to the protected resource, wherein the token (111, 112) is associated with one or more authorized users;

identifying one or more authorized users associated with the detected token (111, 112) who are authorized to access the protected resource, including at least one supervising user;

authenticating whether a first user requesting access to the protected resource is associated with the detected token (111, 112) and authorized to access the protected resource;

detecting one or more wireless transponders (121, 122) of one or more authorized users associated with the token (111, 112), including at least a transponder (121) of the first user and a transponder (121, 122) of the supervising user of the first user;

applying different combinations of rules to grant or deny the first user to access different types of protected resources based at least on a current system state including tokens (111, 112) connected to the device (100, 200) and the transponders (121, 122) tied to the tokens (111, 112), and a detected change of a number of transponders accessing the protected resources within a token reception area, the different types of protected resources include at least protected applications, protected data and protected devices, and the rules are determined based on at least authentication of the first user associated with the detected token (111, 112), detection of the transponder (121, 122) of the first user, and detection of the transponder (121, 122) of the supervising user; and

providing access to the protected resource to the first user when an applicable combination of rules allows the first user to access the protected resource."

The claims also include a corresponding independent system claim 8.

Reasons for the Decision

The invention

1. In general, the application relates to what is called multi-level authentication.

1.1 It is known to require two levels of authentication before a user can gain access to a protected resource: for instance a password and a token. This is referred to as two-level authentication (see description, page 1, lines 17-29).

1.2 Beyond that, the invention proposes the use of tokens and corresponding wireless transponders (see figure 1). A user, in order to get access to a resource, must connect his token to the computer and have the transponder in the proximity of the token (see page 7, lines 24-32, figure 4). In a typical scenario, users will keep their transponders in their pockets (e.g. on a key ring) while working on the computer. In this scenario, a transponder represents the "presence" of the associated user so that the system can detect when the user leaves the computer and take protective action (e.g. by blocking access).

1.3 Sometimes the "presence" of several transponders is required (hence "multi-level authentication"; see e.g. page 7, last paragraph, figure 4), for instance those of a "normal" and a "supervising" user.

1.4 The invention means to make such a multi-level authentication method more flexible and more secure.

1.5 The invention is stated to achieve this by enabling the specification and enforcement of access rules such as those depicted in the tables on pages 11 and 13. A rule of specific interest is that users may get access to a computer only when a "supervising user" (such as the chief accountant) is present, too (see page 13, rule 4, and text below the table). The description discusses several scenarios and proposes rules addressing the risks in these situations.

1.6 It is disclosed that "the systems checks for any change in [the] number of transponders [...] within the reception area of [the] token" and that "[i]n case of a change in their number", "new rules [...] may be applied". In other words, it is disclosed that a change in the number of present transponders may trigger the application of a different rule (see page 8, lines 27-29, figure 5, no. 510).

The prior art

2. D1 discloses presence-based computer access control of the type relied upon in the application (see abstract and figure 1). It is also disclosed that the presence of a plurality of transponders (paired with the same "plug") may be required (see paragraphs 23 and 63) and that rules are evaluated before access can be granted (see figure 4). The fact that it requires two crucial

actions for a user to obtain access to a resource, namely the insertion of a plug and the presence (and authentication) of an associated transponder, is modelled in terms of state diagrams (see figure 5 and 6 and paragraphs 63 and 64).

Claim construction - what is a "supervising user"?

3. Claims 1 and 8 refer to "a transponder [...] of the supervising user of the first user".

3.1 It is, however, neither claimed nor disclosed how it is determined that a transponder is that of a supervising user. In fact, the claims do not require that this is "determined" at all. Rather, the system administrator may specify that user A is authorised to access a particular resource only in presence of user B because B happens to be the supervisor of A, irrespective of whether this is factually true and, even if so, whether the system administrator retrieved this bit of information from a personnel database or knew it by heart. The invention itself would then only have to check for the presence of A's and B's transponders without also checking the administrative roles of A and B. If B ended up being A's supervisor, the system would not change its behaviour until it was reconfigured to take into account that fact.

3.2 In view of this, the board takes the view that, from the perspective of the claimed system (or method of operating it), the reference to a "supervising user of the first user" is indistinguishable from a mere "second user".

Article 56 EPC

4. The board agrees with the decision under appeal that D1 is a suitable starting point for assessing inventive step.

4.1 D1 does not mention supervising users, let alone disclose that

(a) the rules may require the presence of a "transponder of the supervising user" of another "first" user.

4.2 Also, D1 does not disclose that

(b) different combinations of rules may be applied to different types of resources.

4.3 D1 discloses detecting the events that a transponder appears or disappears from the proximity of the associated plug (see especially paragraph 64), and that the system state changes in response to such events (see figure 6). The board agrees with the examining division that in the different system states different access rules apply (see the decision, point 5 of the reasons; page 6, penultimate paragraph); in the intermediate state users have no access (yet), in the access state they do. D1, however, does not disclose that

(c) different access control rules are applied based on "a detected change of a number of transponders".

5. Regarding (a), the examining division found this to be the only difference between the then claimed invention and D1 (see the decision, point 4.2 of the reasons).

5.1 As argued above, the board is not convinced that the required presence of a "supervising user" is a feature of the claimed method or system at all, since the administrative hierarchy between the owners of two required transponders need not, according to the claims, be checked by the method or represented in the system.

5.2 If it was assumed, for the sake of argument, that the "supervising user" constituted a feature of the claimed method and/or system, the board would agree with the examining division (see points 4.3 and 4.4 of the reasons) that this was a non-technical difference. The hierarchy between two users A and B can be changed by an administrative act without any impact on the functioning of the claimed system or method of operating it. The board notes that the appellant did not address this aspect of the decision in its grounds of appeal.

6. Regarding (b), the board considers that, in general, it is a non-technical matter to determine, as a security policy, under which conditions an individual user should or should not have access to a specific resource or "type of resources". Evidently, different resources in a system may have different security requirements.

7. Regarding (c), D1 discloses that the access to a system may require the presence of one or more transponders, depending on the required level of security (see D1, paragraphs 23 and 63). For example, a security policy might prescribe that a user be given access to one resource if one transponder is present and to another resource if two separate transponders are present. If both rules were applied simultaneously, and a required transponder were present, the rules governing the

user's access might change when another transponder appeared or disappeared.

7.1 The appellant correctly notes (see grounds of appeal, page 4, paragraph 3) that the state diagram depicted in figure 6 only relates to a single transponder. However, the skilled person would know that if the presence of several transponders were required, the state diagram would have to be modified so that the "access state" is only entered once all required transponders are detected and it would return to the "intermediate state" as soon as any one of them disappeared. The board considers that this modification of the state diagram and its implementation would be straightforward for the skilled person.

8. In summary, claim 1 - and, by the same token, claim 8 - lacks inventive step over D1, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated