Internal distribution code:

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

Datasheet for the decision of 26 June 2018

Case Number: T 0277/16 - 3.5.06

Application Number: 12189827.4

Publication Number: 2629228

IPC: G06F21/31, G06F21/62

Language of the proceedings: EN

Title of invention:
Location-based security system for portable electronic device

Applicant:
Google LLC

Headword:
Location-based computer access/GOOGLE

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - yes - mixture of technical and non-technical features

Decisions cited:
T 0641/00

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

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 0277/16 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 26 June 2018

Appellant: (Applicant)	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 (US)
Representative:	Maikowski & Ninnemann Patentanwälte Partnerschaft mbB Kurfüstendamm 54-55 10707 Berlin (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 24 September 2015 refusing European patent application No. 12189827.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	A. Teale

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, with reasons dated 24 September 2015, to refuse European patent application No. 12 189 827 because the then main and first auxiliary requests lacked inventive step over

D1: US 2003/0112182 A1

and the second auxiliary request did not comply with Article 123(2) EPC. In the decision, further documents were cited, in particular

D2: US 2010/017874 A1 and
D3: US 2010/0175116 A1,

but not relied upon in its reasons.

II. A notice of appeal was filed on 19 November 2015, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 19 January 2016. The appellant requested that the decision be set aside and that a patent be granted on the basis of claims 1-12 according to the requests which were subject to the refusal, in combination with the application documents on file, namely

description, pages
1-5, 7 and 9 as filed on 18 August 2015,
6, 8 and 10-21 as originally filed, and
figures, no.
1-3 as originally filed.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that

the claimed invention, even though it was non-obvious over D1, lacked inventive step because it did not, as formulated at the time, solve a technical problem.

In response to the summons, with the letter of 23 April 2018, the appellant filed amended claims 1-12 according to a new main and a new auxiliary request, and withdrew auxiliary request 2.

IV. During the oral proceedings, the appellant filed new claims 1-12 as its sole request.

V. The two independent claims 1 and 11 of the main request read as follows:

"1. A method, comprising:

receiving, via an input of a portable electronic device (12), a request to access the electronic device (12);

the electronic device (12) implementing a first security rule requiring a first authentication process when the electronic device (12) is physically located in a familiar area and a different second security rule requiring a different second authentication process when the electronic device (12) is located outside of the familiar area[,] the second authentication process being more complex for the user or requiring more time for the user than the first authentication process; and;

receiving, via an input of the portable electronic device (12), a plurality of successful user authentication entries,

characterized in that the method further comprises:

determining a location of the device (12) corresponding to each of the successful user authentication entries,

wherein determining the location of the device (12) comprises one or more of:

receiving global positioning system data (52) and determining the location based on the global positioning system data (52), and

receiving a network address corresponding to a wireless communications network (22, 32) that the device (12) has detected, and determining the location based on the network address;

saving, in a computer-readable memory, data representative of each of the entries and each entry's corresponding location; and

automatically designating, by a processor without a requirement for user entry of location information, the familiar area for the electronic device (12),

wherein designating the familiar area comprises designating the familiar area based on the data representative of each of the entries and each entry's corresponding location, and

wherein designating the familiar area comprises:

determining a set of successful user authentication entries that were received during a time period,

grouping the entries from the set into a plurality of location-dependent subgroups,

determining a size of the set and a size of each subgroup,

identifying each subgroup having a size that at least equals a size threshold, wherein the size threshold corresponds to a portion of the set size, and

for each subgroup having a size that at least equals the size threshold, classifying the location for that subgroup's entries as the familiar area.

11. An electronic device (12), comprising:

a processor,

a user interface (16), and

a memory having programming instructions that, when executed, instruct the processor to:

receive, via the user interface (16), a user request to access the electronic device (12);

determine a current location for the electronic device (12);

implement a first authentication process if the current location corresponds to a familiar area and a different second authentication process if the current location does not correspond to the familiar area[,] the second authentication process being more complex for the user or requiring more time for the user than the first authentication process;

receive a plurality of successful user authentication entries;

characterized in that the memory further has programming instructions that, when executed, instruct the processor to:

determine a location of the device corresponding to each of the successful user authentication entries,

wherein determining the location of the device (12) comprises one or more of:

receiving global positioning system data (52) and determining the location based on the global positioning system data (52), and

receiving a network address corresponding to a wireless communications network (22, 32) that the device has detected, and determining the location based on the network address;

save data representative of each of the entries and each entry's corresponding location;

output, via the user interface (16), a prompt to perform the implemented authentication process; and

automatically designate, without a requirement for user entry of location information, the familiar area for the electronic device (12);

wherein designating the familiar area comprises designating the familiar area based on the data representative of each of the entries and each entry's corresponding location, and

wherein designating the familiar area comprises:

determining a set of successful user authentication entries that were received during a time period,

grouping the entries from the set into a plurality of location-dependent subgroups,

determining a size of the set and a size of each subgroup,

identifying each subgroup having a size that at least equals a size threshold, wherein the size threshold corresponds to a portion of the set size, and

for each subgroup having a size that at least equals the size threshold, classifying the location for that subgroup's entries as the familiar area."

Reasons for the Decision

The invention

1. The application relates to a location-based access control system balancing computer security and user convenience.

1.1 It is proposed to designate certain physical locations as "familiar" and to require different "security rules" in familiar areas than in other areas. Typical familiar areas may be, for instance, the user's home or work

place. The security rule inside the "familiar area" is meant to be "less complex or less burdensome" for the user than outside it. For example, inside the familiar area a shorter passcode than outside might be required (see page 14, paragraph 2, and page 19, paragraphs 1 and 2). Consequently, logging in in a "familiar" place is less intrusive for the user than elsewhere and, as a consequence, authentication requirements are less intrusive overall.

1.2 The invention further provides an automatic way of "designating" the familiar area. It is proposed to monitor the successful login events and, essentially, to accept every location as familiar where the user has successfully logged in a minimum number of times.

1.3 The system records the GPS location or the network address for every successful login attempt (see page 16, lines 12-16), groups them into logins at the "same" location and then classifies every such group with a minimal number of logins as part of the familiar area (see page 17, lines 7-19).

Clarity, Article 84 EPC, claim construction, and original disclosure, Article 123(2) EPC

2. The term in the claims "familiar area" does not have a specific technical meaning. The claims imply that an area in which a user has successfully authenticated him/herself a number of times is considered to be "familiar". The board takes the view that the term "familiar area" has no meaning beyond that and therefore does not, by itself, limit the claimed invention.

3. The board is satisfied that the present set of claims comply with Articles 84 and 123(2) EPC. Only one feature deserves specific mention.

3.1 Claims 1 and 11 specify that the first and second authentication processes are different from each other and that the second one is "more complex for the user" or "requires more time for the user" than the first one.

3.2 The description discloses that the authentication process used in the familiar area is "less complex or less burdensome" or to require less time than that used elsewhere. It is unambiguously clear from the examples (see page 14, paragraph 2, and page 19, paragraphs 1 and 2) that this refers to "complexity", "burden" and "time" *for the user* as opposed, in particular, to computational complexity, i.e. complexity *for the processor*. The corresponding clarification of the present independent claims thus complies with Article 123(2) EPC.

3.3 The board appreciates that this language implies little detail of the two authentication processes in question. It does however make clear that they must differ specifically in terms of device usability. Hence, although the feature is very broad, it achieves its purpose within the claim of establishing that the adaptive determination of the familiar areas improves device usability. Consequently the board accepts the feature as clear.

The prior art

4. D1 discloses a device which changes access control parameters according to the device location. The

general idea is that in secure zones (such as the user's home) a more lenient security policy should apply than in less secure zones (such as public areas; see paragraphs 2 and 7). The device location is determined by a "location sensor" or via the network connection, and it is determined whether the device is located in one of several user-defined "zones" such as the user's "home" or "work" zone or in an airport or hotel zone (see paragraphs 7 and 14-16). An "access protocol" is associated with every zone which defines *inter alia* certain login requirements. For instance, it might define whether a screen saver may lock the system and thus require re-authentication, or how often this happens (see again paragraph 16).

5. D2 discloses a device that automatically detects its location (e.g. via GPS) and grants or denies user access based on this location. An employee, for instance, might be granted access to a company computer only in the company's building or in the user's home town (see paragraph 5). The relevant zone(s), the location detection mechanism and the associated access policy are predefined (see paragraph 18). It is disclosed that access can further be regulated by external factors, such as the number of requests or the time or date of access and that the access policy can be different for different users (see paragraphs 19 and 33).

6. D3 discloses a system that grants or denies a user's request to perform certain operations via a portable electronic device on the basis of that user's usage characteristics as defined in a usage profile (see paragraph 36). An access attempt which does not fit the expected usage profile, for example an attempt to

withdraw an exceptionally large amount of money at a remote location, may be recognized as suspicious and protected by "further authentication procedures" (see paragraphs 63 and 77, but also figure 3, nos. 320, 325, 330, 335). Conversely, authentication requirements may be reduced if the usage profile indicates that the user has performed a desired activity at a particular location before (see paragraph 85). The usage profile may define where and when the authorized user typically accesses its device, which environmental signals (e.g. cellular or WiFi) are typically received at that point and which programs and data are most often used in a given environment (see e.g. paragraphs 39, 41, 60 and 79). In order to create or modify a usage profile, a "learn mode" is activated, either on express user instruction or automatically after successful user authentication (see figure 1, and e.g. paragraphs 37 to 42, 80 and 86). Parameters measured or input during learn mode may then be used to update the usage profile (*loc. cit.*).

Inventive step

7. In the decision under appeal, the examining division assessed inventive step starting from D1, found that the claimed invention differed from D1 in that a familiar area was automatically determined and how, and thus considered the objective technical problem to be solved by the claimed invention as being "how to define a familiar zone [...] automatically [...]" (see points 7.2 to 7.3 of the reasons).

8. However, D1 discloses that zones are user-defined and does not suggest that it could be otherwise (specifically, the first full sentence of page 2, right column,

does not say that security zones are only "typically user-defined" but that they are "user-defined" and that typical ones are e.g. "home", "work" and "airport").

8.1 The zones in D1 are predefined according to policy decisions in view of "security concerns" (see paragraph 2). For instance, a company might or might not decide that an employee's home is safe (or, at least, safer than a "public place") and that, consequently, the employee should profit from more lenient login requirements at home than in a hotel room or an airport. These zones are meant to be fixed - although some flexibility will have to be provided to account for developments such as users moving house or changing their preferred hotels.

8.2 In contrast, the familiar area as claimed may change over time according to a learning process and its extent does not depend on the security of the locations involved. For instance, the user's preferred coffee shop might, according to the invention, become a "familiar area" over time even though it is a public place with little security.

8.3 This is not to say that the invention ignores security considerations entirely. The authentication requirements in a new location are only relaxed once it can be assumed, in view of repeated successful authentication "entries", that the user is actually authorized, and the electronic device has not been stolen. This is, however, a different security concern than that addressed in D1.

8.4 Therefore, the skilled person addressing the problem of automatically determining the zones of D1 would not, without exercising inventive activity, consider the

claimed manner of automatically determining a familiar area depending on usage patterns, let alone based on successful logins.

8.5 The board is also unaware of an objective technical problem which would naturally arise in the context of D1 and which the skilled person would solve, without exercising inventive activity, by providing the claimed solution.

9. Therefore, the board considers that document D3 provides the best starting point for the assessment of inventive step amongst the documents on file.

9.1 D3 discloses (see references above) that a portable electronic device may require different authentication processes in view of typical usage patterns, "learned" from actual usage, at authorized locations measured e.g. via GPS, and wherein the authentication process may be less complex or require less time for the user at "familiar locations"; see paragraph 85).

9.2 D3 also discloses that authorized locations - which correspond to the "familiar" area in the sense of the claims - are typically defined by radial distance around the device location detected in learn mode, for instance around a fixed GPS location or an access point (see paragraphs 47, 48 and 60), and that there may be several authorized locations per user and device, i.e. that the "familiar" area may extend over several physical locations (see e.g. paragraph 80).

9.3 D3 does not disclose that the familiar area is learned from - and may vary with - the frequency and proximity of "successful user authentication entries" at clusters

(groups) of measured GPS locations or detected network access points.

10. The board considers that this feature increases the convenience of authorized users when using their electronic devices, and thus provides a new access method balancing user convenience and security considerations.

10.1 This is substantially the same difference that the examining division found to exist over D1 and considered to be a straightforward implementation of a "non-technical policy" (see the decision under appeal, points 7.3 and 7.4 of the reasons). Implicitly, this argument was applying the so-called COMVIK approach based, in particular, on T 641/00, headnotes I and II.

10.2 While the board agrees that the difference implements a "policy", it disagrees that it is a *non-technical* policy which does not contribute to inventive step.

10.3 The invention provides a non-intrusive and seamless way of changing device behavior, based on its physical location and its user-dependent actual access history. The distinguishing features are thus intimately tied to the use and usability of the device for the legitimate user and therefore contribute to the technical character of the invention as a whole (see T 641/00, headnote I). In particular, the distinguishing features address the very real technical problem of preventing device access should it be stolen and taken to a location where the legitimate user has never authenticated him/herself to the device. The board judges, accordingly, that achieving the effect of the distinguishing features cannot be treated as an aim to be achieved in a non-technical field which, according

to T 641/00, headnote II, may legitimately appear in the formulation of the objective technical problem.

11. Returning to D3, and in view of the fact that D3, too, discloses access methods balancing user convenience and security considerations, the objective technical problem solved by the invention over D3 may be considered as providing an alternative computer access method striking such a balance. However, in the board's view, D3 does not suggest the criteria according to which the familiar area is determined by the distinguishing features depending on user-dependent actual device usage (see point 9.3 above).

12. The board also considers that D2 cannot suggest the claimed invention. The zones according to D2 are generally fixed, such as those of D1 (see e.g. paragraph 22), even though access in these zones may further depend on dynamic factors such as "number of requests" or a daily policy (see paragraph 19). Moreover, D2 does not explain what the "number of requests" are. Specifically, D2 does not disclose or suggest that these are successful authentication requests by the same user in a certain time period, nor how the "number of requests" affects whether an access request is granted or not. Therefore, in the board's view, the claimed invention would be non-obvious for the skilled person in view of D2.

13. The board thus concludes that claims 1 and 11 involve an inventive step over the prior art on file.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the examining division to grant a patent on the basis of the following documents:

claims, no.
1-12 as filed on 26 June 2018,
description, pages
1-5, 7 and 9 as filed on 18 August 2015,
6, 8 and 10-21 as originally filed, and
figures, no.
1-3 as originally filed.

The Registrar: The Chairman:

I. Aperribay W. Sekretaruk

Decision electronically authenticated