UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/569,816	12/15/2014	Karl Klug	2013P00045US-880	1010

88087 7590 03/03/2020
Fritzsche Patent
c/o Buchanan Ingersoll & Rooney PC (SEN)
P. O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	**PAPER NUMBER**
2431	
NOTIFICATION DATE	**DELIVERY MODE**
03/03/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPDOC1@BIPC.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte KARL KLUG and JURGEN TOTZKE

Appeal 2018-005691
Application 14/569,816
Technology Center 2400

Before BRADLEY W. BAUMEISTER, LINZY T. McCARTNEY, and JASON M. REPKO, *Administrative Patent Judges*.

REPKO, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Under 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 10–29. Appeal Br. 12.[2] An oral hearing was conducted on February 12, 2020. We have jurisdiction under 35 U.S.C. § 6(b). We REVERSE.

CLAIMED SUBJECT MATTER

The claimed subject matter relates to mobile-device security. Spec. 1. In particular, the invention allows a user to configure a device's security level. *See, e.g.*, *id.* at 25. The device's applications have a minimum application security (MAS). *Id.* at 16. The MAS is the security level required to activate an application on the device. *Id.*

For instance, when the user starts an application, the system compares the application's MAS with the mobile device's security level. *Id.* at 26. If the MAS conforms to the device's security level, the application starts. *Id.* Otherwise, the system keeps the application inactive and offers the user a conforming security level for the device. *Id.* According to the Specification, the system allows for situational security and raises the user's awareness about the device's security. *Id.* at 27.

[1] We use the word *Appellant* to refer to *applicant* as defined in 37 C.F.R. § 1.42(a). According to Appellant, "The real party in interest is Unify GmbH & Co. KG, which was formerly known as Siemens Enterprise Communications GmbH & Co. KG." Appeal Br. 1.

[2] Throughout this opinion, we refer to the Final Office Action ("Final"), mailed June 15, 2017; the Appeal Brief ("Appeal Br."), filed October 19, 2017; the Examiner's Answer ("Ans."), mailed May 2, 2018; and the Reply Brief ("Reply Br."), filed May 15, 2018.

Claims 10, 24, and 29 are independent. Claim 10 is reproduced below.

> 10. A method for the handling of security settings of a mobile end device comprising:
>
> determining, by a mobile end device, a minimum application security level required for running a first application prior to activating the first application to run the first application, the mobile end device having a processor and non-transitory memory;
>
> in response to determining that the first application is intended to be run by the mobile end device and that a security level of the mobile end device is below the minimum application security level, emitting output via the mobile end device to facilitate initiation of a change in the security level at which the mobile end device is operating to permit the mobile end device to run the first application;
>
> adjusting the security level at which the mobile end device is operating from a first security level to a higher second security level that meets or exceeds the minimum application security level of the first application in response to receiving input responsive to the emitted output to actuate the adjusting of the security level at which the mobile end device is operating; and
>
> activating the first application to run the first application after the security level of the mobile end device is adjusted from the first security level to the second security level such that the first application is kept inactivated and not run while the mobile end device operates at a security level that is below the minimum application security level.

Appeal. Br. 32, Claims Appendix.

REFERENCES

The Examiner relies on the prior art listed in the table below.

Name	Reference	Date
Baentsch	US 2011/02388994 A1	Sept. 29, 2011
Blaisdell	US 2012/0210443 A1	Aug. 16, 2012
Dumont	US 9,286,482 B1	Mar. 15, 2016

REJECTIONS

The Examiner rejects claims 10–20 and 22–29 under 35 U.S.C. § 103 as unpatentable over Blaisdell and Dumont. Final 7–20.

The Examiner rejects claim 21 under 35 U.S.C. § 103 as unpatentable over Blaisdell, Dumont, and Baentsch. Final 20–21.

OPINION

Claim 10

As noted above, claim 10 recites, in part,

> in response to determining that the first application *is intended to be run* by the mobile end device and that a security level of the mobile end device is below the minimum application security level, emitting output via the mobile end device to facilitate initiation of a change in the security level at which the mobile end device is operating to permit the mobile end device to run the first application.

Appeal. Br. 32, Claims Appendix (emphasis added).

The Rejection of Claim 10

In the obviousness rejection, the Examiner finds that Dumont emits an output in response to a determination that a first application "is intended to be run." Final 8–9. In the Examiner's view, the recited phrase "is intended to be run" is an intended use. Ans. 4; Final 9. As for the recited emitted output, the Examiner finds that Dumont sends a notification when the system detects an unknown user. Ans. 6.

Appellant's Argument

Appellant argues that the Examiner's rejection is based on an incorrect interpretation of the phrase "is intended to be run." Appeal Br. 16–17; Reply Br. 3–4, 8. According to Appellant, the phrase "is intended to be run" is not an intended use. Appeal Br. 16–17. Appellant argues that, under the correct interpretation, claim 10 requires a determination about an application that causes an emitted output, which Dumont lacks. *Id.* at 16–17, 23–24; Reply Br. 8. According to Appellant, Dumont protects the primary user's information from an unknown user. Appeal Br. 23–24. And, in Appellant's view, Dumont would not output the primary user's security settings to the unknown user. *Id.* at 24.

Issue

Under § 103, has the Examiner erred by finding that Dumont teaches or suggests emitting the recited output "in response to determining that the first application is intended to be run by the mobile end device and" that the device's security level is below the MAS, as recited in claim 10?

Analysis

For the reasons below, we determine that the Examiner erred.

In claim 10, the phrase "is intended to be run" limits the recited "determining" step. In particular, the claimed method determines whether the first application is intended to be run. And in response to this determination, the method emits an output. So the phrase "is intended to be run" also limits when the output is emitted.

Under this interpretation of claim 10, the rejection does not adequately address how Dumont teaches or suggests emitting an output in response to the recited determination. Specifically, Dumont's recognition module 102 detects the current user's identity. Dumont 5:17–21. In doing so, recognition module 102 outputs a probability that the current user is the primary user or another known or unknown user. *Id.* That is, Dumont's recognition module 102 makes a determination about the *user*, not about an *application*, as required by claim 10. *See id.* Thus, the Examiner has not shown that Dumont teaches or suggests emitting an output in response to the recited determination.

Nor has the Examiner shown that it would have been obvious to modify Blaisdell with Dumont to obtain the recited determination and associated output steps. For the other limitations, the Examiner cites Blaisdell's application-security process. *See* Final 7–10. Like Blaisdell, the claimed output helps secure the device from applications. But Blaisdell lacks the recited determination and associated output—specifically, an output that allows "a change in the security level at which the mobile end device is operating to permit the mobile end device to run the first application." *Id.* at 8.

Dumont's system would not have remedied this deficiency. Rather, Dumont has a different purpose: protecting the primary user's data from other users. Dumont 5:26–40. For example, Dumont's notification may cause the security module 104 to hide the primary user's data and applications. *Id.* Showing the primary user's security settings to an unknown user would defeat Dumont's data-protection scheme. *Accord* Appeal Br. 24. Thus, the Examiner has not shown how Dumont would have supplied the determination and associated output missing from Blaisdell.

Thus, the Examiner has not shown that Dumont, alone or in combination, teaches or suggests emitting the output in response to the determination recited in claim 10. *See* Final 7–10. So we do not sustain claim 10's rejection.

The Remaining Claims Rejected as Obvious over Blaisdell and Dumont

Independent claims 24 and 29 recite determinations similar to those in claim 10. The Examiner rejects claims 24 and 29 under the same rationale as claim 1. *See* Final 7–8. So for the same reasons, we also do not sustain the rejections of claims 24 and 29.

For the same reasons, we also do not sustain the rejections of claims 11–20, 22, 23, and 25–28, which depend from claims 10, 24, and 29.

The Obviousness Rejection over Blaisdell, Dumont, and Baentsch

We also do not sustain the rejection of dependent claim 21. Specifically, the Examiner did not rely on Baentsch to teach the features missing from Dumont. *See* Final 20–21. Thus, the Examiner has not shown that Baentsch cures the deficiency in the Blaisdell-Dumont combination. *See id.* So the Examiner erred for the same reasons discussed for claim 10's rejection.

CONCLUSION

The Examiner's decision rejecting claims 10–29 is reversed.

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
10–20, 22–29	103	Blaisdell, Dumont		10–20, 22–29
21	103	Blaisdell, Dumont, Baentsch		21
Overall Outcome				10–29

REVERSED