Trials@uspto.gov
571-272-7822

Paper 9
Entered: December 22, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

BLACKBERRY LTD.,
Patent Owner.

Case IPR2017-01619
Patent 8,489,868 B2

Before SALLY C. MEDLEY, ROBERT J. WEINSCHENK, and AARON W. MOORE, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

DECISION
Instituting *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Google LLC ("Petitioner") filed a Petition for *inter partes* review of claims 1, 13, 76–95, 98, 100, 104, 108, 112, 113, 137–39, and 142–44 of U.S. Patent No. 8,489,868 B2 (Ex. 1001, "the '868 patent"). Paper 1 ("Pet."). BlackBerry Ltd. ("Patent Owner") filed a Preliminary Response. Paper 8 ("Prelim. Resp.").

Institution of an *inter partes* review is authorized by statute when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a); *see* 37 C.F.R. § 42.108.

Upon consideration of the Petition, we conclude there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of all of challenged claims 1, 13, 76–95, 98, 100, 104, 108, 112, 113, 137–39, and 142–44 of the '868 patent in this proceeding.

A. Related Matters

According to Petitioner, the '868 patent is at issue in *BlackBerry Ltd. v. BLU Products, Inc.*, No. 1-16-cv-23535 (S.D. Fla.). Pet. 1.

Petitioner concurrently filed another petition, IPR2017–01620, for *inter partes* review of the '868 patent based on different prior art. Pet. 1. The 1620 petition does not challenge claims 87, 108, 138, 143, and 144.

Patent Owner is presently prosecuting a continuation of the '868 patent, U.S. Serial No. 13/413,173, not identified by either party.

B. The '868 Patent

The '868 patent is directed to "a code signing system and method" said to be "particularly well suited for Java™ applications for mobile communication devices, such as Personal Digital Assistants, cellular telephones, and wireless two-way communication devices." Ex. 1001, 1:20–24. The patent explains that "[i]n a typical software code signing scheme, a digital signature is attached to a software application that identifies the software developer" and "[o]nce the software is downloaded by a user, the user typically must use his or her judgment to determine whether or not the software application is reliable, based solely on his or her knowledge of the software developer's reputation." *Id*. at 1:30–36. The patent identifies two drawbacks to this prior art scheme, that it "does not ensure that a software application written by a third party for a mobile device will properly interact with the device's native applications and other resources" and that "[b]ecause typical code signing protocols are not secure and rely solely on the judgment of the user, there is a serious risk that destructive . . . software applications may be downloaded and installed onto a mobile device." *Id.* at 1:37–43.

The solution to these problems described in the '868 patent is "[a] code signing system [that] operates in conjunction with a software application having a digital signature." *Id.* at 1:54–56. "The API[1] is configured to link the software application with [an] application platform" and "[a]virtual machine verifies the authenticity of the digital signature in

---

[1] "API" stands for "application programming interface." Ex. 1001, 1:57.

order to control access to the API by the software application." *Id.* at 1:58–61.

The main embodiment of the '868 patent is described with reference to Figure 1:

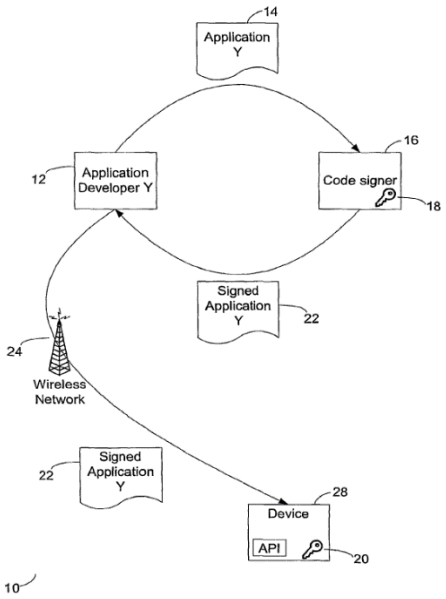

Figure 1

Figure 1 represents "a code signing protocol according to one embodiment of the invention." Ex. 1001, 2:54–55.

As illustrated, "[a]n application developer 12 creates a software application 14 (application Y) for a mobile device that requires access to one or more sensitive APIs on the mobile device." *Id.* at 3:9–12. Then, "[s]oftware application Y 14 is sent from the application developer 12 to the code signing authority 16." *Id.* at 4:24–26. "If the code signing authority 16 determines that software application Y 14 may access the sensitive API and therefore should be signed, then a signature . . . for the software application Y 14 is generated by the code signing authority 16 and appended to the software application Y 14." *Id.* at 4:36–40. "The signed software

application Y 22 may then be sent to a mobile device 28 or downloaded by the mobile device 28 over a wireless network 24" and, "[o]nce the signed software application Y 22 is loaded on the mobile device 28, each digital signature is preferably verified with a public signature key 20 before the software application Y 14 is granted access to a sensitive API library." *Id.* at 4:56–58, 4:66–5:3. "When the signatures are verified, the software application Y 14 can be executed on the device and access any APIs for which corresponding signatures have been verified." *Id.* at 5:9–11.

The '868 patent also describes a method for "network operators" to "maintain control over which software applications are activated on mobile devices." *Id.* at 1:44–46. "In this multiple-signature scenario, all APIs are restricted and locked until a "global" signature is verified for a software application." *Id.* at 4:1–3.

C. Illustrative Claims

Independent claims 1 and 76 are reproduced below, illustrating the claimed subject matter:

> 1. A mobile device containing software instructions which when executed on the mobile device cause the mobile device to perform operations for controlling access to an application platform of the mobile device, the operations comprising:
>
> storing a plurality of application programming interfaces (APIs) at the mobile device, wherein at least one API comprises a sensitive API to which access is restricted;
>
> receiving, at the mobile device, an indication that a software application on the mobile device is requesting access to the sensitive API stored at the mobile device;
>
> determining, at the mobile device, whether the software application is signed, wherein a signed software application includes a digital signature generated using a private key of a

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.