Trials@uspto.gov
571-272-7822

Paper 34
Entered: January 10, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

INTELLECTUAL VENTURES II, LLC,
Patent Owner.

Case IPR2016-01404
Patent 6,968,459 B1

Before THOMAS L. GIANNETTI, PATRICK M. BOUCHER, and KAMRAN JIVANI, *Administrative Patent Judges.*

JIVANI, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Unified Patents Inc. (“Petitioner”) sought *inter partes* review of claims 1, 2, 13–15, 18, 33, 34, 39, 46, and 48 of U.S. Patent No. 6,968,459 B1 (“the ’459 patent”), owned by Intellectual Ventures II, LLC (“Patent Owner”). Paper 2 (“Petition” or “Pet.”). Patent Owner filed a Preliminary Response. Paper 8 (“Prelim. Resp.”). Upon consideration of the Petition and Preliminary Response, we instituted an *inter partes* review of claims 1, 2, 13, 14, 33, 34, 39, 46, and 48 (the “Instituted Claims”) pursuant to 35 U.S.C. § 314. Paper 9 (“Decision on Institution” or “Dec. on Inst.”). We did not institute, however, review of claims 15 and 18 because we determined that Petitioner had not established a reasonable likelihood it would prevail with respect to those claims. *Id.*

During the trial, Patent Owner filed a Patent Owner Response (Paper 19, “PO Resp.”) and observations on cross examination (Paper 30). Petitioner filed a Reply to the Patent Owner Response (Paper 23, “Reply”) and a reply to Patent Owner’s observations (Paper 31). An oral hearing was conducted on November 14, 2017. The record contains a transcript of the hearing (Paper 33, “Tr.”).

We have jurisdiction under 35 U.S.C. § 6. The evidentiary standard is preponderance of the evidence. *See* 35 U.S.C. § 316(e); *see also* 37 C.F.R. § 42.1(d). This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed below, Petitioner has failed to show by a preponderance of the evidence that any of the Instituted Claims are unpatentable.

II. BACKGROUND

A. The '459 patent (Ex. 1001)

The '459 patent seeks to create "a highly secure computing environment . . . preventing the appropriation of sensitive data." Ex. 1001, 1:13–31. The '459 patent describes "a secure computing environment in which a computer automatically operates in a secure 'full access' data storage mode when the computer detects the presence of a secure removable storage device." *Id*. at 1:35–39. If, however, the computer detects the presence of a removable storage device that is not secure, "then the computer automatically operates in a 'restricted-access' mode." *Id*. at 1:39–42. Figure 1 of the '459 patent is reproduced below.

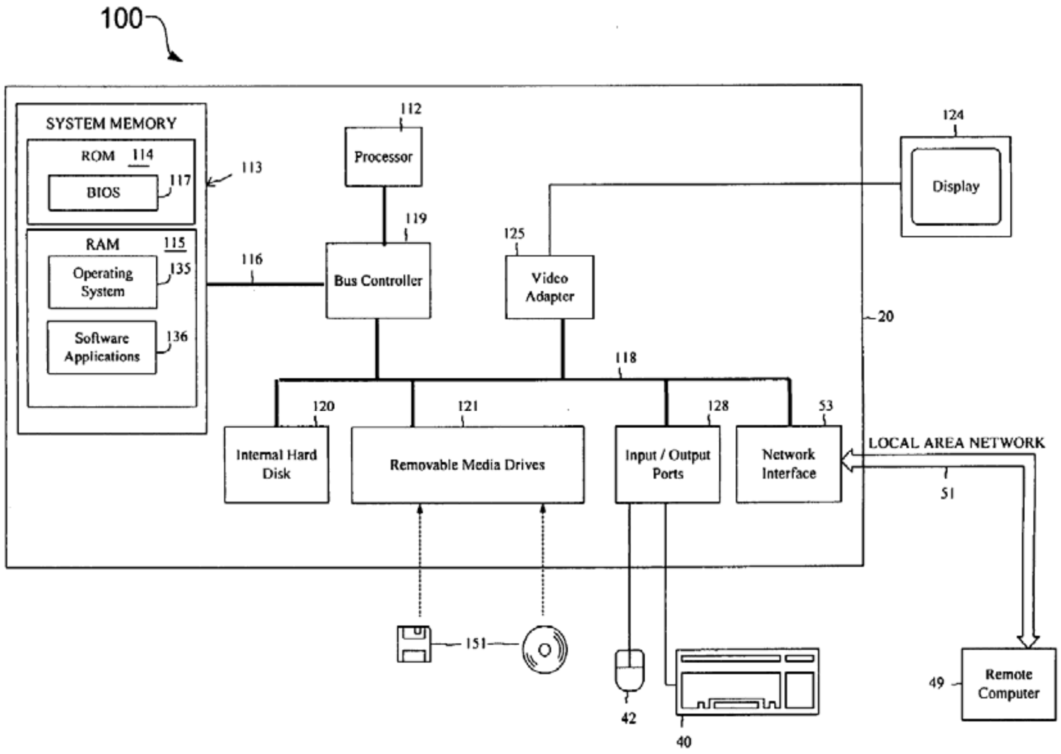

FIG. 1

Figure 1 of the '459 patent depicts a block diagram of a secure computing environment, including computer 100, which senses whether storage device 151 is secure. *Id*. at 1:30–33. To determine whether a removable storage device is secure, the ’459 patent describes attempting to read “device-specific security information” from the storage device. *Id.* at 5:7–10. The device-specific security information is “derived from the unique format information of the removable storage device.” *Id*. at 3:65–4:1. The ’459 patent elaborates:

> In one embodiment, the device-specific security information is a function of the low-level format information and, therefore, uniquely identifies the underlying media of storage device 151. For example, in one embodiment the device-specific security information is a hash of the addresses of the bad sectors for storage device 151. Because it is a function of the physical characteristics of the actual storage medium within storage device 151, the format information is inherently unique to each storage device 151. In other words, the addresses of the bad sectors change from device to device.

Id. at 4:9–19.

According to the ’459 patent, when a computer operates in a secure “full access” data storage mode, storage management software encrypts and decrypts data transmitted between the computer and the removable storage device using a cryptographic key. *Id*. at 3:61–64. The system of the ’459 patent generates this cryptographic key by combining any number of the following types of information: “(1) device-specific security information . . . , (2) manufacturing information that has been etched onto the storage device, (3) drive-specific information, such as drive calibration parameters, retrieved from the storage drive, and (4) user-specific information such as a password or biometric information.” *Id*. at 3:65–4:5.

When a computer operates in a “restricted-access” data storage mode, the computer operates the storage device as “read-only” such that the user may read data from the device but may not write any data to the device. *Id*. at 1:63–66. Alternatively, the user may be permitted "to write the non-sensitive data to the removable storage device in an unencrypted format." *Id*. at 1:66–2:2.

B. Illustrative Claim

Claims 1, 15, 18, 33, and 39 are independent. Claim 1 illustrates the claimed subject matter and is reproduced below.

> 1. A method comprising:
>
> sensing whether a storage device has device-specific security information stored thereon;
>
> operating a computer in a full-access mode when the storage device has the device-specific security information, wherein in the full-access mode the computer permits both read and write access to the storage device; and
>
> operating the computer in a restricted-access mode when the storage device does not have the device-specific security information, wherein in the restricted-access mode the computer permits read access to the storage device and prevents write access to the storage device.

C. Evidence Relied Upon

Petitioner relies on the following references:

1. Bensimon et al., U.S. Patent No. 5,533,125, issued July 2, 1996 (Ex. 1004, "Bensimon").
2. Takahashi et al., U.S. Patent No. 5,825,878, issued Oct. 20, 1998 (Ex. 1005, "Takahashi").
3. Kimura, U.S. Patent No. 5,237,609, issued Aug. 17, 1993 (Ex. 1006, "Kimura").

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.