Trials@uspto.gov
571-272-7822

Paper 10
Entered: June 22, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETAPP, INC., LENOVO (UNITED STATES) INC., and EMC CORP.,
Petitioner,

v.

INTELLECTUAL VENTURES II, LLC,
Patent Owner.

Case IPR2017-00467
Patent 6,968,459 B1

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

JIVANI, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

I. INTRODUCTION

NetApp, Inc., Lenovo (United States) Inc., and EMC Corporation (collectively, "Petitioner") requested an *inter partes* review of claims 15, 18, 24, and 25 (the "Challenged Claims") of U.S. Patent No. 6,968,459 B1 ("the '459 patent"). Paper 1 ("Petition" or "Pet."). Patent Owner Intellectual Ventures II, LLC filed a Preliminary Response. Paper 9 ("Prelim. Resp.").

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless it is determined that there is "a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Based on the information presented in the Petition and Preliminary Response, we are not persuaded that there is a reasonable likelihood Petitioner would prevail on its challenges. Accordingly, we decline to institute *inter partes* review of claims 15, 18, 24, and 25 for the reasons set forth below.

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 1:36–39. 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 1:41, 42. Figure 1 of the '459 patent is reproduced below.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

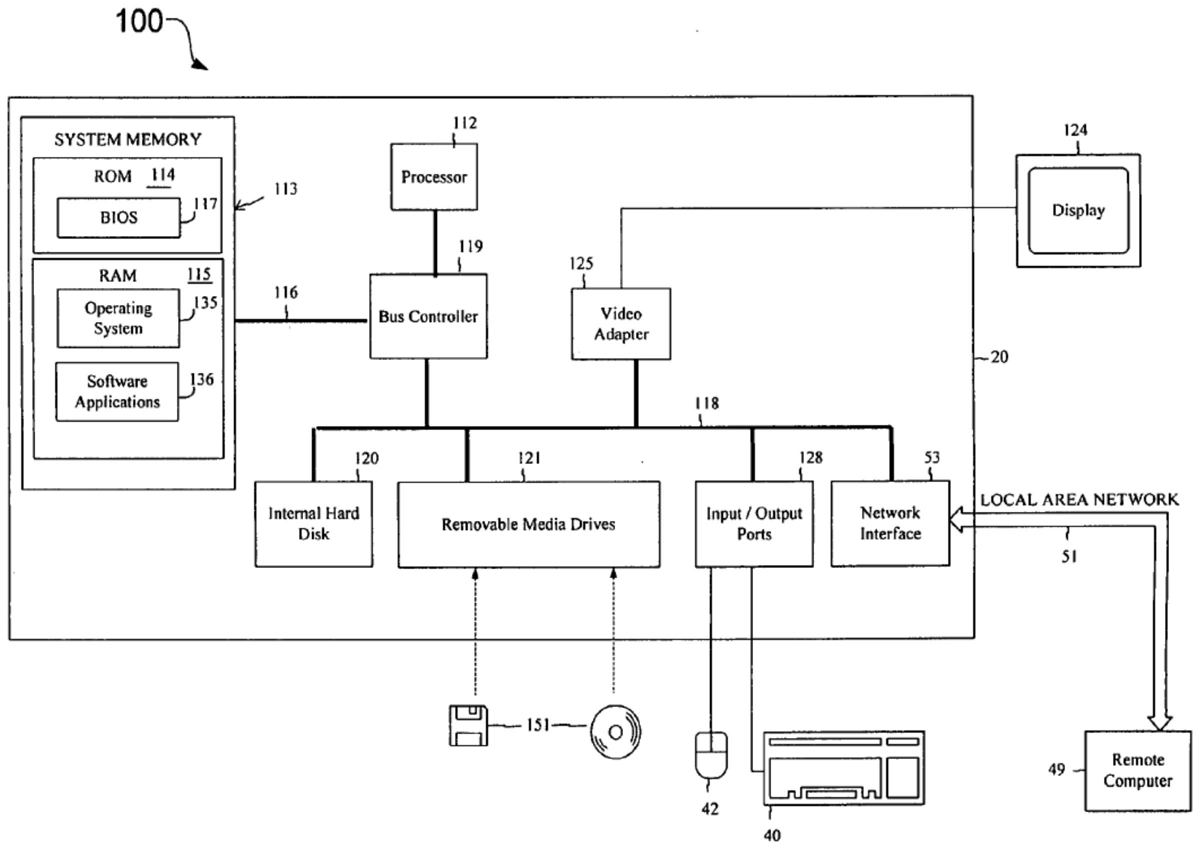

FIG. 1

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 3:66–4:1. 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

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

> 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 [] non-sensitive data to the removable storage device in an unencrypted format." *Id*. at 2:1, 2.

B. Illustrative Claim

Claims 15 and 18 are independent claims. Claim 15 is reproduced below.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

> 15. A method for accessing a storage device comprising:
>
> detecting a storage device within the storage drive;
>
> sensing whether a storage device has device-specific security information stored thereon;
>
> providing full-access to the storage device when the storage device has the device-specific security information by:
>
> > encrypting digital data using the security information during a write access to write the digital data to the storage device; and
> >
> > decrypting digital data using the security information during a read access to read the digital data from the storage device; and
>
> providing restricted-access to the storage device when the storage device does not store the device-specific security information by preventing the digital data from being written to the storage device during the write access.

C. *Evidence Relied Upon*

Petitioner relies on the following references:

1. Blakley III et al., U.S. Patent No. 5,677,952, issued October 14, 1997 (Ex. 1005, "Blakley");
2. Uchida, U.S. Patent No. 7,124,301 B1, issued on October 17, 2006 (Ex. 1006, "Uchida"); and
3. Ian D. Bramhill & Mathew Sims, Copyright in a Digital Age, BT Technol. J. Vol. 15 No. 2 (April 1997) (Ex. 1007, "Bramhill").

Petitioner further relies on the Declaration of Dr. Paul Franzon (Ex. 1002).

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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**