Trials@uspto.gov
571-272-7822

Paper 47
Entered: June 30, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SYMANTEC CORPORATION,
Petitioner,

v.

THE TRUSTEES OF COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK,
Patent Owner.

Case IPR2015-00375
Patent 8,074,115 B2

Before HOWARD B. BLANKENSHIP, BRYAN F. MOORE, and ROBERT J. WEINSCHENK, *Administrative Patent Judges.*

MOORE, *Administrative Patent Judge.*

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

I. INTRODUCTION

We have jurisdiction to hear this *inter partes* review under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed herein, Petitioner has shown by a preponderance of the evidence that claims 1, 3–8, 11, 13–18, 21,

22, 24–29, 32, 34–39, and 42 of U.S. Patent No. 8,074,115 B2 are unpatentable.

A. Procedural History

Symantec Corporation filed a Petition requesting an *inter partes* review of claims 1–42 of U.S. Patent No. 8,074,115 B2 (Ex. 1001, "the '115 Patent"). Paper 2 ("Pet."). In response, Patent Owner, The Trustees of Columbia University in The City of New York, filed a Preliminary Response. Paper 10 ("Prelim. Resp."). Upon consideration of the Petition and Preliminary Response, we instituted an *inter partes* review of claims 1–42, pursuant to 35 U.S.C. § 314. Paper 13 ("Dec.").

Subsequent to institution, Patent Owner filed a Corrected Patent Owner Response (Paper 44 ("PO Resp.")) and Petitioner filed a Reply (Paper 34 ("Pet. Reply")).

An oral hearing was held on March 16, 2016, and a transcript of the hearing is included in the record (Paper 46 ("Tr.")).

B. Related Proceeding

The '115 Patent is involved in the following lawsuit: *Trustees of Columbia University of New York v. Symantec Corp.*, No. 3:13-cv-808 (E.D. Va.). Pet. 1.

C. The '115 Patent

The '115 Patent describes a way to detect "anomalous program executions that may be indicative of a malicious attack or program fault." Ex. 1001, 3:13–15. As disclosed in the '115 Patent, an anomaly detector

trains a model of normal program behavior and applies the model to detect deviations from normal program behavior during subsequent operation. *Id.* at 3:50–56. The anomaly detector of the '115 Patent specifically focuses on detecting deviations in function calls made by the program in order to detect anomalous behavior. *Id.* at 3:46–56. The anomaly detector first "models normal program execution stack behavior." *Id.* at 3:50–52. This behavior may include function names, function call arguments, stack frames, and the like. *Id.* at 3:38–40. The anomaly detector then observes subsequent function calls made by the program and uses the trained model to detect deviations from normal behavior. *Id.* at 3:52–56. In some embodiments, upon identifying a function call as anomalous, the anomaly detector notifies an application community running the same program or same portion of the program that an anomalous function call has been identified. *Id.* at 18:57–59.

The anomaly detector detects a function call being made by a program. The anomaly detector then compares the detected function call to a model of normal function calls computed based on training data. To train a model of normal function calls, the anomaly detector monitors normal execution of the program. Once the model is trained, it is applied against further executions of the program to identify anomalous function calls associated with the program. Thereafter, detected function calls can be compared to the model at step 804 to identify whether the function call is anomalous at step 806. *Id.* at 3:46–56.

D. Illustrative Claim

Of the challenged claims, claims 1, 11, 21, 22, 32, and 42 are the independent claims.

Claim 22, reproduced below, is illustrative.

> 22. A method for detecting anomalous program executions, comprising:
>
> modifying a program to include indicators of program-level function calls being made during execution of the program;
>
> comparing at least one of the indicators of program-level function calls made in an emulator to a model of function calls for at least a part of the program; and
>
> identifying a function call corresponding to the at least one of the indicators as anomalous based on the comparison.

Ex. 1001, 21:50–59.

E. Prior Art Relied Upon

Petitioner relies upon the following prior art references:

Arnold et al.	US 5,440,723	Aug. 8, 1995	(Ex. 1007)
Agrawal et al.	US 8,108,929 B2	Jan. 31, 2012	(Ex. 1008)
Khazan et al.	US 2005/0108562 A1	May 19, 2005	(Ex. 1010)

F. Grounds of Unpatentability

We instituted an *inter partes* review of claims 1–42 on the following grounds:

Challenged Claims	Basis	References
22, 25–29,[1] 32, 35– 39, and 42	§ 102(e)	Khazan
1, 4–8, 11, 14–18, and 21[2]	§ 103(a)	Khazan and Arnold
2, 3, 9, 10, 12, 13, 19, 20, 23, 24, 30, 31, 33, 34, 40, and 41	§ 103(a)	Khazan, Arnold, and Agrawal

I. ANALYSIS

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see also In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1278 (Fed. Cir. 2015)

---

[1] Claim 26 was not included as part of this ground but this appears to be a typographical error because claim 26 depends from claim 22 and contains a limitation essentially the same as claim 36 included in this ground. Therefore, we include claim 26 in this ground. We also apply Petitioner's explanations on pages 27 and 28 of the Petition to claim 26 as well as claim 36.

[2] Claim 26 is listed by Petitioner as included in this challenge but it depends from claim 22 not claim 21 so it is more properly analyzed in the ground including claim 22 based on Khazan.

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.