

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

SYMANTEC CORPORATION,

Petitioner

- vs. -

THE TRUSTEES OF COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK,

Patent Owner

Patent No. 8,074,115

Issued: Dec. 6, 2011

Inventors: Salvatore J. Stolfo, Angelos D. Keromytis, and Stelios Sidiroglou
Title: METHODS, MEDIA AND SYSTEMS FOR DETECTING ANOMALOUS
PROGRAM EXECUTIONS

Inter Partes Review No. _____

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO.
8,074,115 UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. §§ 42.1-.80, 42.100-.123**

Mail Stop Patent Board
Patent Trial and Appeal Board
P.O. Box 1450
Alexandria, VA 22313-1450

December 5, 2014

TABLE OF CONTENTS

	Page
I. INTRODUCTION.....	1
II. MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1))	1
A. Real Party-In-Interest (37 C.F.R. § 42.8(b)(1)).....	1
B. Notice of Related Matters (37 C.F.R. § 42.8(b)(2))	1
C. Designation of Lead and Backup Counsel (37 C.F.R. § 42.8(b)(3)).....	2
D. Service of Information (37 C.F.R. § 42.8(b)(4))	2
III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A))	2
IV. IDENTIFICATION OF CHALLENGE (37 C.F.R. § 42.104(B))	2
A. Effective Filing Date of the '115 Patent.....	2
B. There Is a Reasonable Likelihood That at Least One Claim of the '115 Patent Is Unpatentable Under 35 U.S.C. §§ 102 or 103.....	3
V. OVERVIEW OF THE '115 PATENT.....	4
VI. CONSTRUCTION OF THE CHALLENGED CLAIMS (37 C.F.R. § 42.104(B)(3)).....	7
VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	11
A. The subject matter of the '115 patent is disclosed in the prior art.....	11
1. U.S. Patent Publication No. 2005/0108562 (“Khazan”).....	11
2. U.S. Patent No. 8,108,929 (“Agrawal”)	14
3. U.S. Patent No. 5,440,723 (“Arnold”).....	15
B. Reasons the Claims are Unpatentable.....	17

TABLE OF CONTENTS
(Continued)

	Page
1. Ground 1: Khazan Anticipates Claims 22, 25, 27-29, 32, 35-39, and 42 Under pre-AIA 35 U.S.C. § 102(e)	17
a. Claim 22: “A method for detecting anomalous executions”	17
b. Claim 32: “A non-transitory computer-readable medium containing computer-executable instructions that, when executed by a processor, cause the processor to perform a method for detecting anomalous program executions”	18
c. Claim 42: “A system for detecting anomalous program executions, comprising: a digital processing device”	19
d. Claims 22, 32, and 42: “modifying a program to include indicators of program-level function calls being made during execution of the program”	20
e. Claims 22, 32, and 42: “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”	22
f. Claims 22, 32, and 42: “identifying a function call corresponding to the at least one of the indicators as anomalous based on the comparison”	23
g. Claims 25 and 35: “modifying the function call so that the function call becomes non-anomalous”	24
h. Claims 27 and 37: “the comparing compares the function call name and arguments to the model”	24

TABLE OF CONTENTS
(Continued)

	Page
i. Claims 28 and 38: “the model reflects normal activity of the at least a part of the program”	25
j. Claims 29 and 39: “the model reflects attacks against the at least a part of the program”	26
k. Claim 36: “generating a virtualized error in response to the function call being identified as being anomalous”	27
2. Ground 2: Khazan in View of Arnold Renders Obvious Claims 1, 4-8, 11, 14-18, 21, and 26 Under pre-AIA 35 U.S.C. § 103(a).....	28
a. Claim 1: “A method for detecting anomalous program executions”	29
b. Claim 11: “A non-transitory computer-readable medium containing computer-executable instructions that, when executed by a processor, cause the processor to perform a method for detecting anomalous program executions”	29
c. Claim 21: “A system for detecting anomalous program executions, comprising: a digital processing device”	29
d. Claims 1, 11, and 21: “executing at least a part of a program in an emulator”	29
e. Claims 1, 11, and 21: “comparing a function call made in the emulator to a model of function calls for the at least a part of the program”	30
f. Claims 1, 11, and 21: “identifying the function call as anomalous based on the comparison”	31

TABLE OF CONTENTS
(Continued)

	Page
g. Claims 1, 11, and 21: “upon identifying the anomalous function call, notifying an application community that includes a plurality of computers of the anomalous function call”	32
h. Claims 4 and 14: “modifying the function call so that the function call becomes non-anomalous”	35
i. Claims 6 and 16: “the comparing compares the function call name and arguments to the model”	35
j. Claims 7 and 17: “the model reflects normal activity of the at least a part of the program”	35
k. Claims 8 and 18: “the model reflects attacks against the at least a part of the program”	35
3. Ground 3: The Combination of Khazan, Arnold, and Agrawal Renders Obvious Claims 2, 3, 9, 10, 12, 13, 19, 20, 23, 24, 30, 31, 33, 34, 40, and 41 Under pre-AIA 35 U.S.C. § 103(a)	35
a. Claims 2, 12, 23, and 33: “creating a combined model from at least two models created using different computers”	37
b. Claims 3, 13, 24, and 34: “creating a combined model from at least two models created at different times”	38
c. Claims 9, 19, 30, and 40: “randomly selecting the model as to be used in the comparison from a plurality of different models relating to the program”	39

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.