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

SUPPLEMENTAL DECLARATION OF DR. MICHAEL T. GOODRICH

I, Michael T. Goodrich, Ph.D., declare as follows:

1. I have been asked by Symantec Corporation ("Petitioner") to provide this supplemental declaration with my expert opinions in support of the above-captioned *inter partes* review of U.S. Patent No. 8,074,115 (the "'115 patent").

2. The purpose of this declaration is to clarify my opinions related to issues raised in my deposition for the above-captioned IPR, and to respond to issues raised by the Patent Owner.

3. In addition to the documents mentioned in my earlier declaration, I reviewed the follow documents:

a. Columbia's Patent Owner Response for the above-captioned *inter partes* review of the '115 patent ("Response");

b. Declaration of George Cybenko, Ph.D. In Support of Columbia's Patent Owner Response (Ex. 2030);

c. Declaration of Scott M. Lewandowski (Ex. 2031);

d. Transcript of Deposition of Scott M. Lewandowski, December 4, 2015 (Ex. 1013);

e. Transcript of Expert Deposition of George Cybenko, Ph.D., December 10, 2015 (Ex. 1014); and

f. Galen Hunt, et al., "Detours: Binary Interception of Win32 Functions," Proceedings of the 3rd USENIX Windows NT

Symposium, Seattle, WA, July 1999 (Ex. 1016).

4. I currently hold the opinions set forth in this declaration.

5. I understand that the Patent Owner in its Response for IPR2015-00375, and through its expert, Dr. Cybenko, states that a person of ordinary skill in the art (POSITA) at the time of the invention of the '115 patent would have at least an undergraduate degree in computer science or mathematics and one to two years of experience in the field of computer security. Response at 4; Ex. 2030 at ¶¶ 24-28. Patent Owner contrasts this level of skill with my previously stated opinion that the level of ordinary skill in the art of the '115 patent at the time of the effective filing date is a person with a Master's degree in computer science or a related field with two to three years of experience in the field of software security systems. *See* Ex. 1003 at ¶ 20.

6. The primary distinction between Dr. Cybenko and my stated opinions is whether the person of ordinary skill has a Master's degree or an undergraduate degree. *See* Ex. 1014 at 25:1-9. A typical Master's degree in computer science or a related field requires one to two years of study. Thus, the difference in the levels of ordinary skill opined by me and Dr. Cybenko is as little as one to two years of schooling or experience in the field.

7. In my opinion, this one to two year difference is not material to the understanding of the technologies and concepts expressed in the '115 patent and its

claims. Accordingly, the opinions I previously expressed using the higher level of skill in the art still hold if Dr. Cybenko's asserted lower level of ordinary skill in the art is used. Hence, my opinions with respect to the claims of the '115 patent do not change if Patent Owner's asserted level of ordinary skill in the art is adopted by the Board. *See* Ex. 2029 at 312:15-22 ("all of my conclusions still hold with [Patent Owner's] definition of a person of ordinary skill").

8. Khazan discloses a model of typical computer system usage. Khazan in its Background section recognizes that "[a]nomaly detection approaches use a model or definition of what is expected or normal with respect to a particular application and then look for deviations from this model." Ex. 1010 at ¶ 8. Here, Khazan is using "expected or normal with respect to a particular application" to refer to "typical computer system usage." Khazan then uses consistent terminology when describing its own model. Specifically, Khazan says that the model produced by its static analyzer comprises "the identified calls, their locations within the program, and other call related information." Ex. 1010 at ¶ 114. The model is used to "distinguish between normal or expected behavior of code and the behavior produced by MC [malicious code]…If the run time behavior deviates from the application model, it is determined that the application executable has executed MC." *Id.* at ¶ 65. Khazan's application model thus describes "normal or expected behavior of the code," which is the behavior one would expect the code to follow during

typical computer system usage. *See id.* at ¶ 67 ("Normal behavior, or non-MC behavior, is associated with particular target function calls identified by the static analyzer 104."). Because the model describes "normal or expected behavior of the code" (i.e., typical computer system usage), Khazan is able to use the model to determine that the application executable has executed malicious code "[i]f the run time behavior deviates from the application model" Ex. 1010 at ¶ 65.

9. Khazan discloses "executing at least part of a program in an emulator," where the "emulator" permits both monitoring and selective execution of certain parts, or all, of the program. As I discussed in my earlier declaration, Khazan discloses that the dynamic analysis may be emulated or simulated. Ex. 1003 at ¶ 66; Ex. 1010 at ¶¶ 110-112 ("An execution of the application may also be emulated or simulated."). The emulation described in Khazan is performed by an emulator. This emulator permits both monitoring and selective execution of certain parts, or all, of the program.

10. I understand that Patent Owner argues, and Dr. Cybenko testifies, that the "emulated" execution in Khazan would not permit monitoring and selective execution. Response at 18-20; Ex. 2030 at ¶¶ 131-53. Dr. Cybenko states that "one possible meaning of the term 'emulate' in general computing…is 'to imitate the functions of (another computer system) by means of software.'" Ex. 2030 at ¶ 138 (quoting Ex. 2042 at 3). While I generally agree with this definition, the conclu-

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.