Trials@uspto.gov
571-272-7822

Paper 8
Entered: March 25, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUNIPER NETWORKS, INC.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

Case IPR2019-00031
Patent 8,141,154 B2

Before THOMAS L. GIANNETTI, MIRIAM L. QUINN, and PATRICK M. BOUCHER, *Administrative Patent Judges.*

QUINN, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Juniper Networks, Inc. ("Petitioner") filed a Petition to institute *inter partes* review of claim 1 of U.S. Patent No. 8,141,154 B2 (Ex. 1001, "the '154 patent"). Paper 2 ("Pet."). Finjan, Inc. ("Patent Owner") timely filed a Preliminary Response. Paper 7 ("Prelim. Resp.").

We have jurisdiction under 35 U.S.C. § 314. For the reasons discussed below, we do not institute *inter partes* review of claim 1 of the '154 patent.

A. Related Matters

The parties indicate that the '154 patent is involved in *Finjan, Inc. v. Juniper Networks, Inc.*, Case No. 3:17-cv-05659-WHA (N.D. Cal.) and other proceedings. Pet. 1; Paper 5.

B. The '154 Patent (Ex. 1001)

The '154 patent relates to computer security, and, more particularly, to systems and methods for protecting computers against dynamically generated malicious code, such as viruses that enter a computer over the Internet. Ex. 1001, 1:7–9, 34–37, 8:38–40. The '154 patent identifies two types of anti-virus applications that are available to protect against internet viruses: gateway security applications that shield web content before it is delivered to a computer, and desktop security applications that shield web content after it is delivered to the computer. *Id.* at 1:43–53. Each system has its disadvantages. *Id.* at 2:31–45. Gateway security applications fail to detect certain types of viruses, such as viruses that are generated dynamically at run-time of a computer program. *Id.* at 3:31–36. Desktop security applications may be able to shield dynamically generated viruses;

however, these applications require the installation of client computer software and can be vulnerable to hackers. *Id.* at 4:15–22.

With regard to the embodiment shown in Figure 2, reproduced below, the '154 patent describes shielding a client computer from dynamically generated malicious code by passing the input of a function to a security computer for inspection before the client computer invokes the function. *Id.* at 4:35–43, 8:41–44.

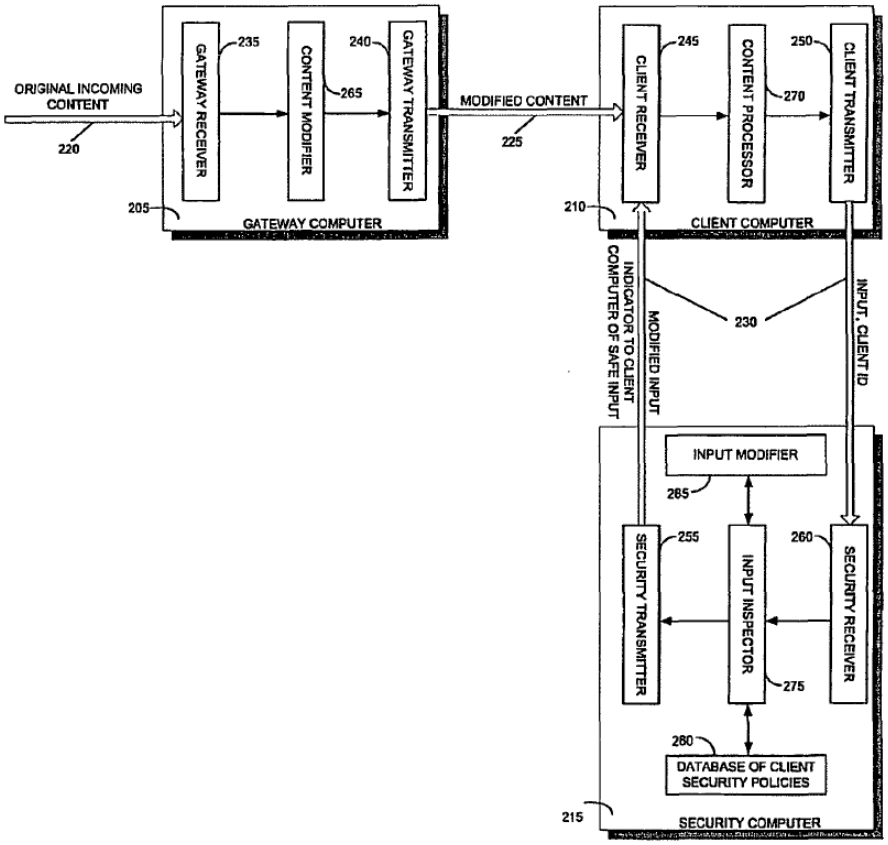

FIG. 2

Figure 2 depicts a system for protecting a computer from dynamically generated malicious executable code, including gateway computer 205, client computer 210, and security computer 215. *Id.* at 8:45–47. The gateway computer 205 receives content from a network, such as the Internet,

over communication channel 220. *Id.* at 8:47–48. "Such content may be in the form of HTML pages, XML documents, Java applets and other such web content that is generally rendered by a web browser." *Id.* at 8:48–51. Client computer 210 communicates with gateway computer 205 over communication channel 225, and communicates with security computer 215 over communication channel 230. *Id.* at 8:51–54. The client computer receives content data at client receiver 245, processes the data at content processor 270, and transmits data at client transmitter 250.

Content modifier 265 modifies original content received by gateway computer 205 and produces modified content that includes a layer of protection to combat dynamically generated malicious code. *Id.* at 9:13–16. Specifically, content modifier 265 identifies certain function calls and replaces them with a substitute function call, and when content processor 270 processes the substitute function, the input is sent to security computer 215 for inspection. *Id.* at 9:16–28, 10:60–64. Input inspector 275 compares the input's security profile to the client computer's security policy. *Id.* at 11:40–41. If the operations of the function violate the client computer's security policy and are potentially malicious, input inspector 275 sets an "inspection_result" value to false and the client computer does not invoke the original function. *Id.* at 11:1–4, 12:20–24. Otherwise, the "inspection_result" value is set to true, and the client computer invokes the original function. *Id.*

C. Illustrative Claim

Challenged claim 1, reproduced below, is independent.

> 1. A system for protecting a computer from dynamically generated malicious content, comprising:

> a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;
>
> a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and
>
> a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

Ex. 1001, 17:32–44.

D. Asserted Prior Art and Grounds of Unpatentability

The Petition identifies the following references in connection with Petitioner's challenge of unpatentability (Pet. 4–5):

a) *Gladstone*: U.S. Patent No. 7,594,267 B2, filed in the record as Exhibit 1006;

b) *Ji*: U.S. Patent No. 5,983,348, filed in the record as Exhibit 1005; and

c) *Chander*: *Mobile Code Security by Java Bytecode Instrumentation*, DARPA Information Survivability Conference and Exposition II, June 12–14, 2001, filed in the record as Exhibit 1008.

Petitioner asserts the following grounds of unpatentability based on the aforementioned references (Pet. 5):

Challenged Claim	Basis	References
1	§ 103(a)	Gladstone and Ji
1	§ 103(a)	Chander and Gladstone

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.