Trials@uspto.gov
Tel: 571-272-7822

Paper 10
Entered: July 31, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

RADWARE INC.,
Petitioner,

v.

F5 NETWORKS, INC.,
Patent Owner.

Case IPR2017-00653
Patent 7,472,413 B1

Case IPR2017-00654
Patent 7,472,413 B1

Before KRISTEN L. DROESCH, TRENTON A. WARD, and DAVID C. McKONE, *Administrative Patent Judges*.

WARD, *Administrative Patent Judge*.

DECISION[1]
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

[1] This Decision addresses the same legal and factual issues raised in IPR2017-00653 and IPR2017-00654. The same patent is at issue in both cases, and many of the arguments made by the parties are the same in both cases. Therefore, we issue one Decision to be entered in both cases.

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

I. INTRODUCTION

A. Background

Radware, Inc. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–24 of U.S. Patent No. 7,472,413 B1 (Ex. 1001, "the '413 patent") pursuant to 35 U.S.C. §§ 311–319. IPR2017-00653, Paper 2 ("Pet.").[2] F5 Networks, Inc. ("Patent Owner") filed a Preliminary Response. IPR2017-00653, Paper 7 ("Prelim. Resp."). With authorization from the Board, Petitioner filed a Reply to Patent Owner's Preliminary Response. IPR2017-00653, Paper 9 ("Reply"). Petitioner also filed a second Petition requesting an *inter partes* review of claims 1–24 of the '413 patent in IPR2017-00654. IPR2017-00654, Paper 2 ("'654 Pet."). Patent Owner filed a Preliminary Response to this second Petition. IPR2017-00654, Paper 7 ("'654 Prelim. Resp."). Also, with authorization from the Board, Petitioner filed a Reply to Patent Owner's Preliminary Response. IPR2017-00654, Paper 9 ("'654 Reply"). We have statutory authority under 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." *See also* 37 C.F.R § 42.4(a) (delegating authority to the Board).

Upon consideration of the Petition, Patent Owner's Preliminary Response, Petitioner's Reply to the Preliminary Response, and the

[2] For clarity and expediency, we treat IPR2017-00653 as representative of IPR2017-00654. Unless indicated otherwise, all citations are to papers and exhibits filed in IPR2017-00653.

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

associated evidence filed in both IPR2017-00653 and IPR2017-00654, we conclude Petitioner has failed to demonstrate a reasonable likelihood in either case that it would prevail with respect to at least one of the challenged claims. Accordingly, for the reasons that follow, we deny institution of an *inter partes* review in both IPR2017-00653 and IPR2017-00654.

B. Related Matters

Petitioner and Patent Owner indicate that Patent Owner asserted the '413 patent against Petitioner in *F5 Networks, Inc. v. Radware, Inc.*, Case No. 16-cv-480-RAJ, in the Western District of Washington. Pet. 1; Paper 3, 1. Patent Owner also indicates that U.S. Patent No. 9,003,509 is a continuation of the '413 patent. Paper 3, 1.

C. The '413 Patent

The '413 patent is titled "Security for WAP Servers" and generally relates to computing software and systems for managing internet website and web application security and for preventing website and web application users from causing harm. Ex. 1001, [54], 1:14–17. The challenged claims relate to creating a model of an application and using that model to validate requests from web clients before the request reaches a web application server. As noted above, Petitioner challenges claims 1–24, of which claims 1, 12, 16, and 23 are independent. Independent claim 1 is representative and reproduced below:

> 1. A method of managing a communication over a network, comprising:
>
> generating an application model based on interactions with an application over the network;

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

intercepting a request to the application from a client to the application residing on a server over the network;

comparing the request to the application model;

if the request is compliant with the application model, forwarding the request to the application;

receiving a response to the request;

examining the response for state data, including at least a hidden field value within the response;

storing the hidden field value;

generating an encrypted state token associated with the stored hidden field value;

inserting the encrypted state token into the response, wherein the encrypted state token and response is sent to the client within a hidden form field of the response, if the response includes a form; within a query string of the response, if the response includes a link; or within a Uniform Resource Locator (URL) path within the response, if the response includes a URL; and

allowing a subsequent request from the client to be forwarded to the application if the subsequent request includes the encrypted state token.

Id. at 17:42–67.

The ’413 patent describes improving the security and control of web applications by intercepting incoming web client requests that are non-compliant with the application model before the request reaches the web application server. *Id.* at Abstr. Figure 6 of the ’413 patent is reproduced below.

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

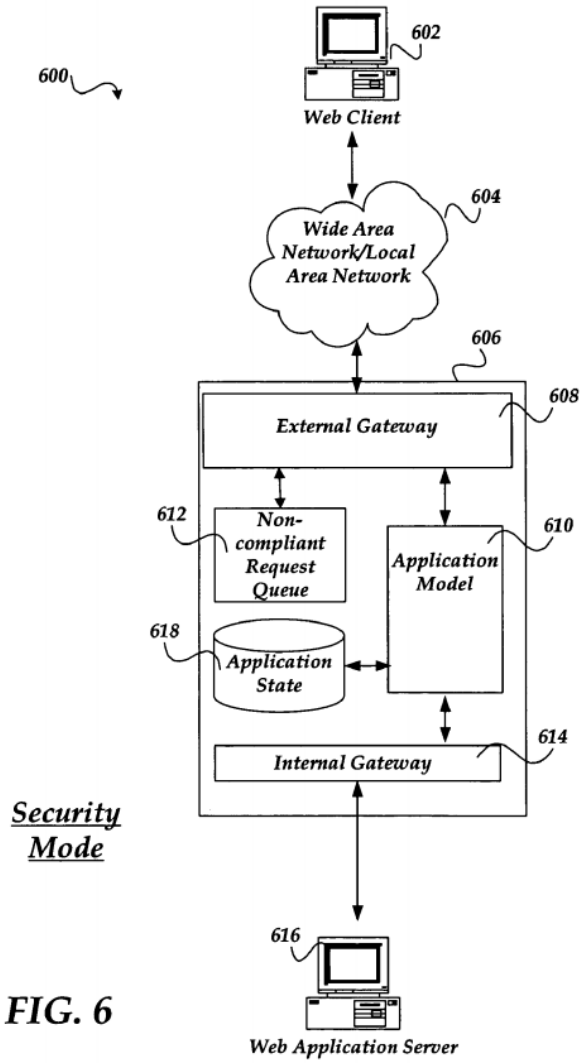

FIG. 6

Id. at Fig. 6. Figure 6 is a functional block diagram of an embodiment of the invention operating in security mode. *Id.* at 8:63–64. As shown above in Figure 6, web application security system 606 is configured to intercept incoming messages from network 604 originating from web client 602, as well as outgoing messages from web application server 616. *Id.* at 8:64–9:3.

The '413 patent discloses generating application model 610 using a "web crawler," which automatically surveys and processes the target application. *Id.* at 3:15–18; *see id.* at 9:42–10:25. Application model 610 may employ application state information to determine if an incoming HTTP

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

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.