Trials@uspto.gov
571.272.7822

Paper No. 11
Filed: October 7, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE MANGROVE PARTNERS MASTER FUND, LTD.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-01046
Patent 6,502,135 B1

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

SIU, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

A. Background

The Mangrove Partners Master Fund, Ltd. ("Petitioner") filed a Petition ("Pet.") on April 27, 2015 (Paper 5) requesting *inter partes* review of claims 1, 3, 4, 7, 8, 10, and 12 of U.S. Patent No. 6,502,135 B1 ("the '135 Patent," Ex. 1001) pursuant to 35 U.S.C. §§ 311-319. VirnetX Inc. ("Patent Owner") filed a Preliminary Response ("Prelim. Resp.") on July 24, 2015. Paper 9.

We have jurisdiction under 35 U.S.C. § 314. We determine based on this record that Petitioner has demonstrated, under 35 U.S.C. § 314(a), that there is a reasonable likelihood of showing unpatentability with respect to at least one of the challenged claims, claims 1, 3, 4, 7, 8, 10, and 12.

Petitioner relies on the following prior art:

Takahiro Kiuchi and Shigekoto Kaihara, *C-HTTP-- The Development of a Secure, Closed HTTP-Based Network on the Internet,* PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, IEEE 64–75 (1996) (Ex. 1002, "Kiuchi").

P. Mockapetris, *Domain Names – Concepts and Facilities*, Network Working Group, Request for Comments: 1034 (1987) (Ex. 1005, "RFC 1034").

Petitioner contends that the challenged claims are unpatentable under 35 U.S.C. § 102 and/or § 103 based on the following specific grounds (Pet. 3–4, 15–37):

Reference(s)	**Basis**	**Claims challenged**
Kiuchi	§ 102	1, 3, 4, 7, 8, 10, and 12
Kiuchi and RFC 1034	§ 103	8

B. The Invention

The ’135 Patent describes a system and method for securely communicating over the Internet. Ex. 1001, 2:66.

Claim 1 of the ’135 Patent is reproduced below:

> 1. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:
>
> (1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;
>
> (2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and
>
> (3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

Ex. 1001, 47:20–32.

We note that the ’135 Patent is presently the subject of co-pending actions, as follows:

1) Civ. Act. No 6:13-cv-00211-LED (E.D. Tex.), filed February 26, 2013;

2) Civ. Act. No. 6:12-cv-00855-LED (E.D. Tex.), filed November 6, 2012;

3) Civ. Act. No. 6:10-cv-00417-LED (E.D. Tex.), filed August 11, 2010.

See Pet. 1.

II. ANALYSIS

A. Cited References

1) Overview of Kiuchi

Kiuchi discloses a closed HTTP-based network ("C-HTTP") for a closed group of institutions, in which each member is protected by its own firewall. Ex. 1002, 64. Communication is made possible with a client-side proxy (for one institution), a server-side proxy (for another institution), and a C-HTTP name server that provides both client-side and server-side proxies with each peer's public key and Nonce values for both request and response. *Id.* at 64–65.

The client-side proxy asks the C-HTTP name server whether it can communicate with the host specified in a given URL. If the connection is permitted, the C-HTTP name server sends the IP address and public key of the server-side proxy and both request and response Nonce values, which are encrypted and certified using asymmetric key encryption and digital signature. *Id.* at 65.

The client-side proxy then sends an encrypted request (including the client-side proxy's IP address, hostname, request Nonce value and symmetric data exchange key for request encryption) to the server-side proxy, which then asks the C-HTTP name server if the query from the client-side proxy is legitimate. *Id.* If the request is confirmed to be legitimate and access is permitted, the C-HTTP name server sends the IP address and public key of the client-side proxy and both request and response Nonce values to the server-side proxy. After receiving the client-side proxy's IP address, hostname and public key, the server-side proxy generates and sends a connection ID to the client-side proxy. After the client-side

proxy accepts the connection ID from the server-side proxy, the connection is established. *Id.* at 66.

2) Overview of RFC 1034

RFC 1034 discloses a name server that answers standard queries in recursive mode or non-recursive mode. Ex. 1005, 22. In non-recursive mode, the server is unable to provide an answer to the request and refers to "some other server 'closer' to the answer." In recursive mode, the server "returns either an error or the answer, but never referrals." *Id.*

B. Claim Construction

We interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1275–79 (Fed. Cir. 2015). We presume a claim term carries its "ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question" at the time of the invention. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) (citation and quotations omitted).

Petitioner and Patent Owner each proffer proposed constructions of several claim terms. For purposes of this decision, we determine that no claim terms require express construction.

C. Kiuchi - Anticipation

Based on the present record at this preliminary stage of the proceedings, we agree that Petitioner has established that there is a reasonable likelihood of unpatentability of at least one claim as anticipated by Kiuchi. For example,

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.