



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 11/485,600 | 07/12/2006 | Matt E. Hart | INTU-060539 | 2442 |
| 63773 | 7590 | 02/02/2015 | EXAMINER | |
| PVF -- INTUIT, INC. c/o PARK, VAUGHAN, FLEMING & DOWLER LLP 2820 FIFTH STREET DAVIS, CA 95618-7759 | | | TURCHEN, JAMES R | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2439 | |
| | | | NOTIFICATION DATE | DELIVERY MODE |
| | | | 02/02/2015 | ELECTRONIC |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jeannie@parklegal.com
kathi@parklegal.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MATT E. HART

Appeal 2012-010717
Application 11/485,600¹
Technology Center 2400

Before JEREMY J. CURCURI, JENNIFER L. McKEOWN, and,
IRVIN E. BRANCH, *Administrative Patent Judges*.

McKEOWN, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1–26. App. Br. 3. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

STATEMENT OF THE CASE

Appellant's invention generally relates to a system that improves security during web-browsing. More specifically, the system receives a URL from the user and queries a DNS server for an IP address for the URL.

¹ The real party in interest is Intuit, Inc.

The system determines a public-key associated with the URL and uses the public-key to encrypt a string that is sent to a remote system. The system can receive a response from the remote system and determine whether the DNS server has been compromised using the response from the remote system. If it is determined that the DNS server has been compromised, the system alerts the user. Abstract.

Claim 1 is illustrative and is reproduced below, with key disputed limitations emphasized:

1. A non-transitory computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for improving security during web-browsing, the method comprising:
 - receiving a Universal Resource Locator (URL) from a user;
 - determining an Internet Protocol (IP) address for the URL by querying a Domain Name Server (DNS) server;
 - determining a public key associated with the URL;
 - encrypting a string using the public key to obtain an encrypted string;
 - sending the encrypted string to a remote system which is associated with the IP address;
 - receiving a response from the remote system;
 - determining that the DNS server has been compromised when the response from the remote system does not match an expected response; and*
 - responsive to determining that the DNS server has been compromised, alerting the user, thereby improving security during web-browsing.

THE REJECTIONS

The Examiner relies upon the following prior art in rejecting the claims on appeal:

Lerat

US 2002/0010627 A1

Jan. 24, 2002

| | | |
|----------|--------------------|--|
| Robotham | US 6,704,024 B2 | Mar. 9, 2004 |
| Dent | US 6,769,060 B1 | July 27, 2004 |
| Kelley | US 2007/0083670 A1 | Apr. 12, 2007 (filed Oct. 11, 2005) |

Claims 8–13 and 20–24 stand rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Ans. 4–5.

Claims 1, 2, 4–9, and 11–26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Dent, Kelley, and Lerat. Ans. 5–9.

Claims 3 and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Dent, Kelley, Lerat, and Robotham. Ans. 9.

THE 35 U.S.C. § 101 REJECTION

Appellant here presents no arguments with respect to the rejection of claims 8–13 and 20–24 under 35 U.S.C. § 101. Moreover, Appellant suggests that they are not contesting that rejection at this point. *See* Reply Br. 3 (“For the purposes of this appeal, *and without admission as to the appropriateness of the other grounds raised by the Examiner*, Appellants will address the Examiner’s reliance on Dent and Kelley in view of Lerat in rejecting independent claims 1, 8, 14, 20, and 25-26 in the instant application under 35 U.S.C. § 103.”)(emphasis added). As such, we summarily affirm the Examiner’s rejection of claims 8–13 and 20–24 under 35 U.S.C. § 101.

THE OBVIOUSNESS REJECTION BASED ON DENT, KELLEY AND LERAT

The Examiner here finds that Dent, Kelley, and Lerat together teach the limitations of claim 1. Ans. 5–7. Appellant, on the other hand, contends that the cited combination fails to teach determining that the DNS server has been compromised when the response from the remote system does not match an expected response.

ISSUE

Does the cited combination of Dent, Kelley, and Lerat teach determining that the DNS server has been compromised when the response from the remote system does not match an expected response, as recited in claim 1?

ANALYSIS

Based on the record before us, we are persuaded that the Examiner erred in rejecting the claims as obvious.

The Examiner here relies on Dent as teaching the disputed limitation — determining whether the DNS server has been comprised when the response from the remote system does not match an expected response. *See* Final Act. 4–5; Ans. 6. The Examiner notes that Dent does not teach a DNS server and relies on Kelley for that limitation. Ans. 6. The Examiner additionally cites Lerat as support for the combination, namely for teaching protecting from DNS spoofing. Ans. 6–7 (citing Lerat ¶¶ 162–163).

Appellant contends that Dent fails to teach the disputed limitation because it is directed to a two-party identity-verification system. App. Br. 10–11. More specifically, “Dent describes a technique for enabling a first

‘party A’ to verify the identity of a second ‘party B’ (and vice versa).” App. Br. 11; *see also* Dent col. 3, ll. 51–52 (“The present invention is a method for bilateral identity authentication over a communication channel.”). In contrast, according to Appellant, the disputed limitation requires three entities or parties, the computer (doing the determining), a DNS server, and a remote system. And the claimed limitation further requires that the computer determine that the DNS server is compromised based on a response from the remote system. App. Br. 11.

We understand that the Examiner finds that Dent teaches the disputed limitation because Dent determines that a remote party cannot be verified. According to the Examiner, this in turn suggests that the DNS server has been compromised. For example, the Examiner finds that “[a]n attempt to connect to the server would be made signing with the public key, and a false server would not contain the private key necessary to return a proper response. This would indicate that there is a man in the middle attack and/or DNS spoofing occurring.” Ans. 7.

We disagree. Instead, we agree with the Appellant that Dent is directed to bilateral identity verification system, in contrast to the claimed invention which is directed to authentication of a DNS server through a remote system. While Dent teaches verifying (or not) a remote party based on that remote party’s response, Dent does not suggest use of a remote party’s response to authenticate a DNS server.

Kelley does not cure the deficiency of Dent. As the Examiner states, Kelley “discloses basic URL -> IP retrieval from a DNS agent that Dent fails to disclose (receiving a URL... determining an IP ...) and a response that a DNS server has been compromised (exposed to suspicion, discredit or

mischief).” Final Act. 2. The mere use of a DNS server to obtain URL addresses does not in turn teach using a remote system response to determine whether the DNS server is compromised.

Therefore, we find that the Examiner erred in rejecting claims 1, 2, 4–9, and 11–26 under 35 U.S.C. § 103(a) as unpatentable over Dent, Kelley, and Lerat.

THE OBVIOUSNESS REJECTION BASED ON DENT, KELLEY,
LERAT, AND ROBOTHAM

As discussed above, we are persuaded that the Examiner erred in rejecting claims 1 and 8, from which claims 3 and 10 depend. The Examiner does not propose Robotham to cure the deficiency of Dent, Kelley, and Lerat. As such, we are similarly persuaded that the Examiner erred in rejecting claims 3 and 10 as unpatentable over Dent, Kelley, Lerat, and Robotham.

CONCLUSION

The Examiner erred in rejecting claims 1–26 as unpatentable over the cited prior art combinations.

DECISION

The Examiner’s decision rejecting claims 1–26 under 35 U.S.C. § 103 is reversed, but the decision rejecting claims 8–13 and 20–24 under 35 U.S.C. § 101 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

Appeal 2012-010717
Application 11/485,600

AFFIRMED-IN-PART

msc