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.
12/675,599	04/22/2010	Trond Lemberg	OSL-068	5392

3897 7590 02/22/2018

Law Offices of Thomas Schneck
P.O. BOX 2-E
SAN JOSE, CA 95109

EXAMINER
DEBNATH, SUMAN

ART UNIT	PAPER NUMBER
2495	

MAIL DATE	DELIVERY MODE
02/22/2018	PAPER

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte TROND LEMBERG

Appeal 2017-009428
Application 12/675,599[1]
Technology Center 2400

Before MAHSHID D. SAADAT, ALLEN R. MacDONALD, and JOHN P. PINKERTON, *Administrative Patent Judges*.

PINKERTON, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 2–15, which constitute all the claims pending in this application. Claim 1 was cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

[1] The real party in interest identified by Appellant is Message Management AS. App. Br. 3.

STATEMENT OF THE CASE

Introduction

Appellant's described and claimed invention relates generally to security mechanisms for message based electronic transactions. *See* Spec. ¶ 1.[2]

Claim 2 is representative and reads as follows (with the disputed limitations *emphasized*):

> 2. A method for *assessment of security in transport paths/routes* used by senders with a declaration of security level of the transport paths/routes in one or more data networks, where the one or more data networks comprise at least one or more senders, at least one or more receivers, at least one or more intermediate nodes characterized in that the method at least comprises the steps of:
>
> a) the at least one or more senders sending a declaration request to an entity being a node intermediate the one or more senders and one or more receivers and independent of the one or more receivers,
>
> b) the entity, in response to the at least one or more senders' declaration request to the entity, verifying at least one messaging service address of the at least one or more receivers identified in the declaration by:
>
> interrogating a domain name server having access to a crawler database of previously established and regularly maintained addressing details of the at least one messaging service address with respect to server names of machines that run at least one messaging service for

[2] Our Decision refers to the Final Office Action mailed May 2, 2016 ("Final Act."), Appellant's Appeal Brief filed December 22, 2016 ("App. Br.") and Reply Brief filed June 21, 2017 ("Reply Br."), the Examiner's Answer mailed April 21, 2017, and the original Specification filed February 26, 2010 ("Spec.").

the at least one or more receivers and at least one address associated with the machines, or

interrogating the crawler database or storage means accessible to the entity where the database or storage means have access to the addressing details of the at least one messaging service address with respect to the server names of the machines that run the at least one messaging service for the at least one receiver and the at least one address associated with the machines, the entity being neither the sender nor the receiver, and

c) *the entity verifying a security level or level of confidentiality of one or more connections requested by the at least one or more senders based upon said addressing details*, and

d) the entity sending a response to the declaration request of the at least one or more senders, the response being a quality statement of the security settings of the receiver,

whereby senders are provided a security level assessment of network transport paths/routes associated with the at least one or more receivers prior to initiating a communication session with the at least one or more receivers.

App. Br. 16–17 (Claims App.).

Rejection on Appeal

Claims 2–15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Polk (US 2008/0133761 A1; published June 5, 2008) ("Polk"), in view of Annic (US 2006/0013157 A1; published Jan. 19, 2006) ("Annic").

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellant's arguments in the Appeal Brief (*see* App. Br. 7–14) and Reply Brief (*see*

Reply Br. 2–6), and are not persuaded the Examiner has erred. Unless otherwise noted, we adopt as our own the findings and reasons set forth by the Examiner in the Office Action from which this appeal is taken (Final Act. 2–15), and in the Examiner's Answer (Ans. 2–7), and we concur with the conclusions reached by the Examiner. For emphasis, we consider and highlight specific arguments as presented in the Briefs.

Appellant argues the combination of cited references fails to teach or suggest a verification of a security level or level of confidentiality associated with one or more network connections to a receiver. *See* App. Br. 9–14; *see also* Reply Br. 2–6. More specifically, Appellant argues Polk merely discloses verifying a security level or a level of confidentiality of a called party rather than a security level or level of confidentiality of a transport route/path (i.e., connection) in a network between an intermediate node and a called party. *See* App. Br. 9–11; *see also* Reply Br. 2. Appellant further argues Annic fails to cure this deficiency of Polk as Annic fails to describe any assessment of security in transport paths/routes or verifying of a security level or level of confidentiality associated with one or more network connects to a receiver. *See* App. Br. 11–12; *see also* Reply Br. 2–4. Appellant also argues Polk and Annic teach (a) a *receiver-centric* verification mechanism where security information is established *synchronously* in relation to an establishment of a communication session by a sender, whereas the claimed invention involves (b) a *sender-centric* verification mechanism where security information is established *asynchronously* in relation to an establishment of a communication session by a sender. *See* App. Br. 13–14; *see also* Reply Br. 5–6.

We are not persuaded the Examiner erred. Regarding Appellant's argument that Polk merely discloses verifying a security level of a called party rather than a security level of a connection to the called party, we agree with the Examiner that the claimed "verifying a security level or level of confidentiality of one or more connections," as recited in independent claim 2 and similarly recited in independent claim 10, when interpreted under the broadest reasonable interpretation, reads on Polk's verifying a security level of a called party. *See* Ans. 2–3. Polk's verification that a called party is authorized to participate in a session at a requested security level is a type of verification of a connection to the called party, and Appellant's claims fail to distinguish the claimed verification from the verification taught in Polk. *See* Polk ¶¶ 58–59. Regarding Appellant's argument that the combination of Polk and Annic fails to teach a sender-centric verification mechanism where security information is established asynchronously in relation to an establishment of a communication session, this argument is not persuasive because claims 2 and 10 fail to recite the aforementioned feature. Thus, we agree with the Examiner that the combination of cited references teaches all the limitations of claims 2 and 10.

Accordingly, we sustain the Examiner's rejection of claims 2 and 10 for obviousness under 35 U.S.C. § 103(a). We also sustain the Examiner's rejection of claims 3–9 and 11–15, which depend from one of claims 2 and 10, and which are not argued separately.

DECISION

We affirm the Examiner's rejection of claims 2–15 under 35 U.S.C. § 103(a).

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).

AFFIRMED