UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

WOWZA MEDIA SYSTEMS, LLC
and COFFEE CUP PARTNERS, INC.
Petitioner

v.

ADOBE SYSTEMS INCORPORATED
Patent Owner

_____

Case IPR2013-00054 (TLG)
Patent 8,051,287 B2

_____

Before HOWARD B. BLANKENSHIP, THOMAS L. GIANNETTI, and
MICHAEL J. FITZPATRICK, *Administrative Patent Judges.*

BLANKENSHIP, *Administrative Patent Judge.*

DECISION
DENYING INTER PARTES REVIEW
37 C.F.R. § 42.108

I. BACKGROUND

Petitioner requests *inter partes* review of claims 1-3, 5, 6, 10, 12-14, 16, 17, 21, 23-26, 28, 29, and 33 of the '287 patent under 35 U.S.C. §§ 311 *et seq*. Patent Owner submitted a preliminary response under 37 C.F.R. § 42.107(b) on February 20, 2013. Paper No. 11. We have jurisdiction under 35 U.S.C. § 314.

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides as follows:

> THRESHOLD -- The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

For the reasons that follow, the Board, acting on behalf of the Director, denies the petition.

A. The '287 Patent (EX 1001)

The challenged patent relates to establishing an encrypted communication session. Figure 1 of the '287 patent is reproduced below.
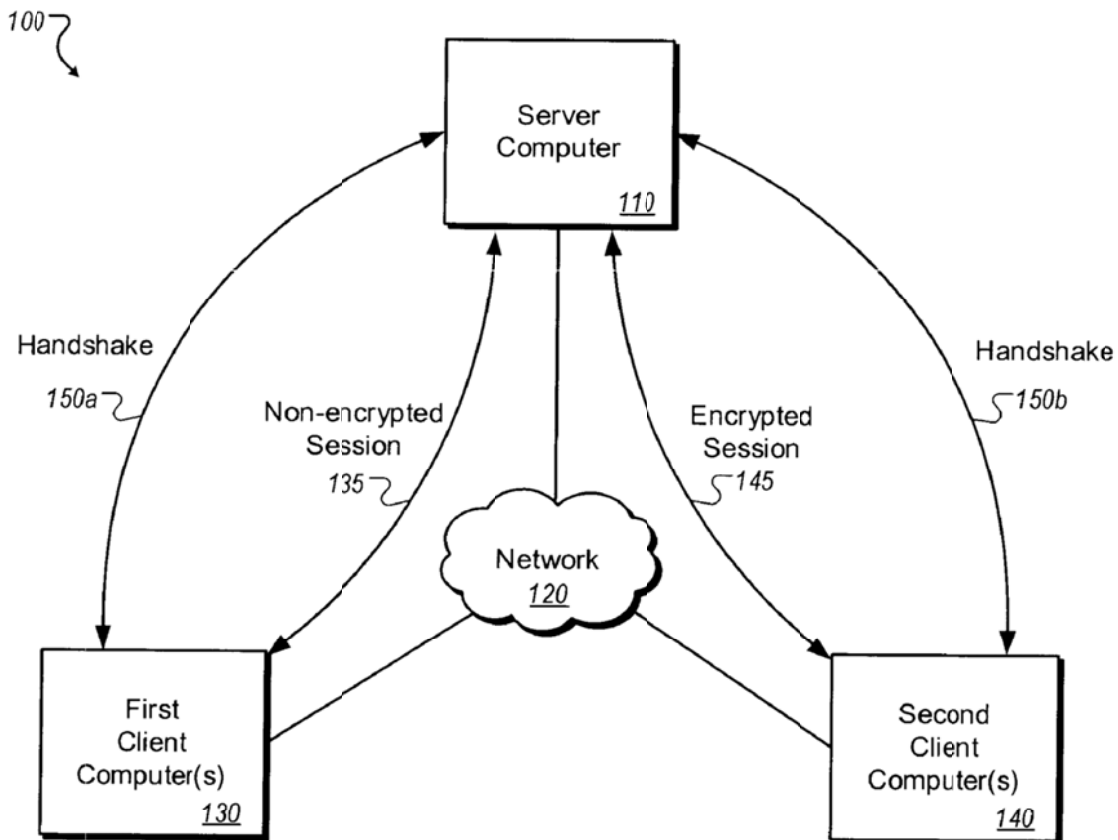
FIG. 1

Figure 1 is said to depict a network environment 100 that includes a server 110 (e.g., a FLASH® Media Server), communicating over a network 120 with a first client computer 130 and a second client computer 140. '287 patent col. 8, ll. 9-15.

Handshakes 150a and 150b precede the sessions 135 and 145 and can include cryptographic information that client 130 may not recognize as such. *Id.* at ll. 15-18. However, the second client computer 140 may include a newer version of software (e.g., a newer FLASH® Player program) that can start an encrypted session 145 with the server computer. *Id.* at ll. 56-59.

Each handshake 150a and 150b may include a block of bytes that contain random data. *Id*. at ll. 25-30. In particular, cryptographic information (e.g., for use in an encryption key establishment protocol) can be included in a previously existing section of the handshake 150 known to contain random bytes, allowing the cryptographic information to be "hidden in plain sight" because the cryptographic information appears to be random. Reverse engineering attempts (i.e., attempts to discover the details of the communication protocol) can thus be handicapped while providing interoperability with existing software. *Id*. at col. 7, l. 67 - col. 8, l. 8; col. 9, ll. 23-46.

B. Representative Claim

Of the challenged claims, claims 1, 10, 12, 21, 23, and 33 are independent. For purposes of this decision, claim 1 is representative. Each of the other independent claims contains the same or substantially similar limitations to those emphasized in claim 1, below. Further, in challenging each of the independent claims, Petitioner relies on the same arguments with respect to the limitations in controversy as represented by claim 1.

> 1. A method comprising:
>
> *establishing, based at least in part on cryptographic information in a pre-defined portion of a handshake network communication*, *a communication session* to communicate a media stream, *wherein the pre-defined portion of the handshake network communication is reserved for random data*;
>
> receiving through the communication session, as part of the media stream, values of parameters relating to a sub media stream, included in a first header portion of a first real-time, priority-based network communication;

storing the values of the parameters;

obtaining through the communication session, as part of the media stream, state information included in a control portion of a second real-time, priority-based network communication and a data payload included in the second network communication;

identifying, from the state information, a purpose of the second network communication in relation to the media stream, and whether a second header portion of the second network communication includes one or more new values corresponding to one or more of the parameters;

updating, when the second header portion includes the one or more new values, one or more of the stored values based at least in part on the one or more new values; and

processing the data payload based at least in part on the identified purpose and the stored values of the parameters.

(Emphasis added.)

C. Claim Construction

As a step in our analysis for determining whether to institute a trial, we determine the meaning of the claims. Consistent with the statute and the legislative history of the AIA, the Board will construe the claims using the broadest reasonable interpretation. *See* Office Patent Trial Practice Guide, 77 Fed. Reg. 48756, 48766 (Aug. 14, 2012); 37 CFR § 100(b). The claim language should be read in light of the specification as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). The Office must apply the broadest reasonable meaning to the claim

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.

fastcase®
Smarter legal research.