IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Kevin J. Ma et al.	
U.S. Patent No.:	9,313,178	Attorney Docket No.: 50095-0082IP1
Issue Date:	April 12, 2016	
Appl. Serial No.:	14/266,368	
Filing Date:	April 30, 2014	
Title:	METHOD AND SYSTEM FOR SECURE OVER-THE-TOP LIVE VIDEO DELIVERY	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 9,313,178 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

EXHIBITS

APPLE-1001	U.S. Patent 9,313,178 to Ma et al. ("the '178 patent")
APPLE-1002	Prosecution History of the '178 Patent (Serial No. 14/266,368)
APPLE-1003	Expert Declaration of Dr. Aviel Rubin, Ph.D.
APPLE-1004	U.S. Pub. 2002/0172368 ("Peterka")
APPLE-1005	U.S. Pub. 2010/0235528 ("Bocharov")
APPLE-1006	European Patent Pub. 1 418 756 A2 ("Chen")
APPLE-1007	U.S. Pub. 2009/0254708 ("Balraj")
APPLE-1008	U.S. Pub. 2012/0254456 ("Visharam")
APPLE-1009	U.S. Pub. 2008/0270308 ("Peterka308")
APPLE-1010	U.S. Pub. 2005/0138362 ("Kelly")
APPLE-1011	U.S. Pub. 2011/0067012 ("Eisen")
APPLE-1012	U.S. Pub. 2011/0099594 ("Chen594")
APPLE-1013	Chow et al., *A White-Box DES Implementation for DRM Applications*, Pre-Proceedings for ACM DRM-2002 Workshop (October 15, 2002)
APPLE-1014	RFC793: *Transmission Control Protocol* (September 1981)
APPLE-1015	RFC2616: *Hypertext Transfer Protocol – HTTP/1.1* (June 1999)

CLAIM LISTING

Element	Claim Language
[1.P]	A method for handling secure distribution of content comprising:
[1.1]	initiating a media playback request and receiving a playback request response;
[1.2]	parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;
[1.3]	retrieving content and manifest files from a content delivery server;
[1.4]	detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;
[1.5]	issuing requests to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached; and
[1.6]	applying the second key for content decryption after the key rotation boundary is reached.
[2]	The method of claim 1, wherein the content encryption keys and content encryption key identifiers returned in the playback request response include the content encryption key and associated identifier currently being applied as well as a future content encryption key and associated identifier yet to be applied.
[3]	The method of claim 1, wherein the content encryption key expiration returned in the playback request response is expressed as an expected minimum interval between periodic key rotation.
[4]	The method of claim 3, further comprising: timing the prefetching of a next un-retrieved content encryption key based on an expected expiration of the content encryption key currently being used.

Element	Claim Language
[5]	The method of claim 4, further comprising: prefetching a next un-retrieved key a fixed duration before the expected expiration of the content encryption key currently being used.
[6]	The method of claim 4, further comprising: prefetching a next un-retrieved key within a period of time after the expected expiration of the content encryption key currently being applied, the period of time beginning at the expected expiration of the content encryption key currently being used, and ending at a duration calculated as a fixed percentage of a fixed periodic content encryption key expiration interval.
[7]	The method of claim 1, wherein subsequent content encryption key identifiers are predictable based on a predetermined known progression.
[8]	The method of claim 7, further comprising: the identifier being calculated as monotonically increasing sequential integer values based on the number of segments or video frames generated during a fixed periodic content encryption key expiration interval.
[9]	The method of claim 7, further comprising: the identifier being calculated as an expected wall clock time for applying the next content encryption key based on a fixed periodic content encryption key expiration interval.
[10]	The method of claim 1, wherein license server communications are secured and authenticated using a selected one of Secure Sockets Layer and a token-based technique using a token encrypted with a symmetric key.
[11]	The method of claim 10, wherein the token-based technique employs white box encryption to encrypt the token.
[12]	The method of claim 1, wherein actual content encryption key rotation boundaries are detected based on real-time in-band notifications.

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.