

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DUO SECURITY INC., CENTRIFY CORPORATION, and
TRUSTWAVE HOLDINGS, INC.,
Petitioner,

v.

STRIKEFORCE TECHNOLOGIES, INC.,
Patent Owner.

Case IPR2017-01041
Patent 8,484,698 B2

Before KERRY BEGLEY, KIMBERLY MCGRAW, and
JOHN A. HUDALLA, *Administrative Patent Judges*.

BEGLEY, *Administrative Patent Judge*.

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

Duo Security Inc., Centrifly Corporation, and Trustwave Holdings, Inc. (collectively, “Petitioner”) filed a Petition requesting *inter partes* review of claims 1–3, 5–7, 15, 20–24, and 48–54 of U.S. Patent No. 8,484,698 B2 (Ex. 1001, “‘698 patent”). Paper 2 (“Pet.”). StrikeForce Technologies, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Pursuant to 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless “the information presented in the petition . . . and any response . . . 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.” Having considered the Petition and the Preliminary Response, we determine that the information presented does not show that there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of any of the challenged claims of the ’698 patent. Thus, for the reasons given below, we deny institution of an *inter partes* review.

I. BACKGROUND

A. RELATED MATTERS

The parties represent that the ’698 patent is the subject of numerous ongoing and completed actions before various district courts. Paper 3, 2–3; Pet. 5. In actions before the U.S. District Court for the District of New Jersey, Patent Owner alleges that Petitioner infringes the ’698 patent (Case Nos. 2:16-cv-03571, 2:16-cv-03573, and 2:16-cv-03574). Paper 3, 2; Pet. 5.

In addition, before the Office, the ’698 patent also is the subject of IPR2017-01064, filed by Petitioner. Pet. 5–6; Paper 3, 2.

B. THE ’698 PATENT

The ’698 patent is directed to security systems that provide user authentication. Ex. 1001, 1:20–25. According to the ’698 patent, prior art authentication systems typically are in-band systems in which data and authentication information are exchanged on a single channel. *Id.* at 2:31–3:14, 5:63–6:12, Fig. 1. To increase security, the ’698 patent instead implements an out-of-band system with “an authentication channel that is separated from the [access] channel carrying the information . . . for actual information transfer.” *Id.* at 3:14–20, 4:52–57, 6:9–23; *see id.* at 1:20–25.

In particular, the '698 patent discloses a multichannel, out-of-band security system for granting or denying access to a host computer in response to a user's access request. *Id.* at [57], 4:34–36. In the first authentication factor, the user seeking access to the host computer presents user identification and password data over an access channel. *Id.* at [57], 4:36–39. This information is intercepted and transmitted to a security computer, which verifies the information. *Id.* at [57], 4:35–36. Next, in the second authentication factor, the security computer communicates with the user through a peripheral device, such as a telephone, within a separate authentication channel. *Id.* at [57], 4:39–42. The security computer authenticates the user via a password entered on the telephone keypad and may further authenticate the user using a biometric system, which controls access based on “characteristics of the human body,” such as fingerprints or voice. *Id.* at [57], 2:13–17, 4:39–46, 6:47–59. Upon obtaining a match, the security computer instructs the host computer to grant access. *Id.* at [57].

One embodiment of the disclosed security system is illustrated in Figure 1A, reproduced below. *Id.* at 5:17–20, 6:30–33, Cert. of Corr.

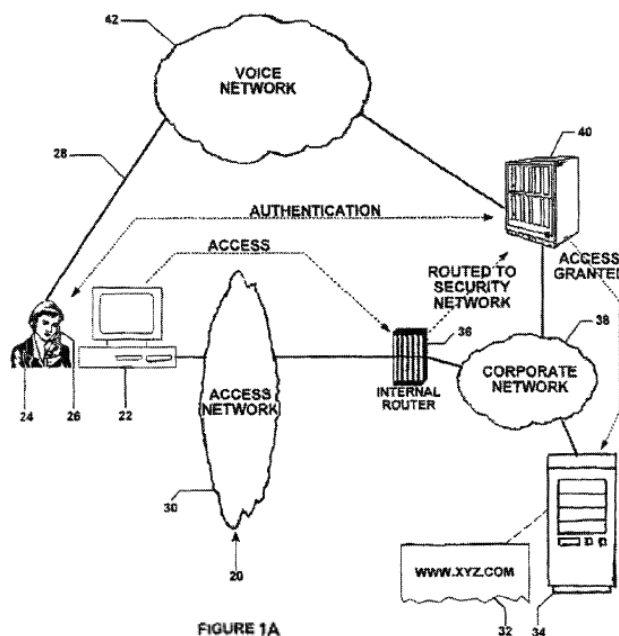


Figure 1A depicts first embodiment 20 applied to a wide area network, such as the Internet, where the user seeking access and its equipment are remote from the host computer. *Id.* at 5:17–20, 6:14–18, 6:30–33; *see id.* at 5:43–45, 6:34–59, 9:10–12:26, Figs. 9A–E. In access network 30, user 24 using remote computer 22 requests access to web page 32 located at host computer 34. *Id.* at 6:33–40, 9:24–27. In the first authentication factor, host computer 34 requests a login procedure in which the user is prompted to enter a user identification and password. *Id.* at 9:27–33. After the user enters this information, router 36, internal to corporate network 38, diverts the information to out-of-band security network 40 containing security computer 52, where authentication occurs. *Id.* at 6:40–42, 6:60–66, 9:33–35. Security computer 52 verifies the password using stored password information. *Id.* at 9:36–54; *see id.* at 7:11–25. Upon verification, security computer 52 sends a verification message to host computer 34, which transmits the message to remote computer 22. *Id.* at 9:55–10:19, Fig. 9B.

In the second authentication factor, security computer 52 initiates an out-of-band telephone call to user 24. *Id.* at 6:35–37, 10:20–30. When the user answers telephone 26, security computer 52 retrieves and plays for the user a prompt to enter a dual tone multi frequency (“DTMF”) password on the telephone keypad. *Id.* at 10:30–48, 15:50–55, 17:19–20. Security computer 52 verifies the DTMF password entered by the user. *Id.* at 10:48–65. Security computer 52 then retrieves and plays for the user a prompt for a speech password. *Id.* at 11:10–37. Using voice recognition technology, security computer 52 verifies that the speech password received from user 24 has the same pattern as a previously stored sample of the user’s speech pattern. *Id.* at 11:26–30, 11:37–42; *see id.* at 6:47–59. After verifying that the stored and received speech patterns match, security

IPR2017-01041

Patent 8,484,698 B2

computer 52 informs the user that access is granted and sends an authentication message to host computer 34. *Id.* at 11:57–12:24. Host computer 34 then grants access to the authenticated user. *Id.* at 12:24–26.

C. ILLUSTRATIVE CLAIM

Of the challenged claims, claims 1, 48, 53, and 54 of the '698 patent are independent. Claim 1, reproduced below, is illustrative:

1. A software method for employing a multichannel security system to control access to a computer, comprising the steps of:
 - receiving at an interception device in a first channel a login identification demand to access a host computer also in the first channel;
 - verifying the login identification;
 - receiving at a security computer in a second channel the demand for access and the login identification;
 - outputting from the security computer a prompt requesting transmission of data;
 - receiving the transmitted data at the security computer;
 - comparing the transmitted data to predetermined data; and
 - depending on the comparison of the transmitted and the predetermined data, outputting an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto.

Ex. 1001, 14:30–46.

D. EVIDENCE OF RECORD

The Petition relies upon the following asserted prior art references:

U.S. Patent No. 5,699,513 (issued Dec. 16, 1997) (Ex. 1003, “Feigen”);
U.S. Patent No. 5,736,932 (issued Apr. 7, 1998) (Ex. 1004, “Bulfer”);
U.S. Patent No. 5,668,876 (issued Sept. 16, 1997) (Ex. 1005, “Falk”); and
International Publication No. WO 99/44114 (published Sept. 2, 1999) (Ex. 1006, “Turtiainen”).

In addition, Petitioner supports its contentions with the Declaration of Patrick McDaniel, Ph.D. (Ex. 1002).

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.