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.
14/623,241	02/16/2015	Jon Arron McClintock	170116-1550	1460

71247 7590 09/18/2019

Client 170101 c/o
THOMAS HORSTEMEYER, LLP
3200 WINDY HILL RD SE
SUITE 1600E
ATLANTA, GA 30339

EXAMINER	
HAILU, TESHOME	
ART UNIT	**PAPER NUMBER**
2434	
NOTIFICATION DATE	**DELIVERY MODE**
09/18/2019	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):

docketing@thomashorstemeyer.com
uspatents@tkhr.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JON ARRON MCCLINTOCK, DARREN ERNEST CANAVOR,
and GEORGE NIKOLAOS STATHAKOPOULOS

Appeal 2018-008679
Application 14/623,241
Technology Center 2400

Before JOSEPH L. DIXON, JAMES W. DEJMEK, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

BELISLE, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–8 and 10–21. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

[1] Throughout this Decision, we use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42 (2017). Appellant identifies the real party in interest as Amazon Technologies, Inc. App. Br. 2.

STATEMENT OF THE CASE

The Claimed Invention

Appellant's invention generally relates to "providing a honeypot environment in response to incorrect credentials being provided for accounts" in an online computer network. Spec. ¶ 8.

According to the Specification, embodiments of Appellant's invention "combat attacks that rely upon guessing security credentials by automatically providing a honeypot environment in certain cases where incorrect credentials are provided." Spec. ¶ 9. The honeypot environment is "configured to be attractive to attackers such that the attackers will devote their time and resources to the honeypot environment instead of a production environment." Spec. ¶ 9. "[T]he honeypot environment will provide access to a fake account in response to an incorrect security credential such that the attackers believe that they have access to a real account." Spec. ¶ 9.

According to the Specification, honeypot selection criteria may control which types of failed login attempts result in providing a honeypot environment and which types of failed login attempts result in providing an error message. Spec. ¶ 25. In an exemplary embodiment, the honeypot selection criteria may specify that access to a honeypot environment is to be provided "if the failed login attempt specifies a credential from compromised credential data" (Spec. ¶ 26), which "may include a list of credentials that are known to be compromised" (Spec. ¶ 29).

Claims 1 and 3 are illustrative of the subject matter on appeal and are reproduced below with the disputed limitations emphasized in *italics*:

> 1. A non-transitory computer-readable medium embodying a program executable in at least one computing device, wherein

when executed the program causes the at least one computing device to at least:

in response to receiving from a client a login request for an account, determine whether the login request specifies an incorrect password;

in response to determining that the login request specifies the incorrect password, determine whether the incorrect password corresponds to a known compromised password; and

in response to determining that the incorrect password corresponds to the known compromised password, provide the client with access to a honeypot environment that is configured to mimic a successful login via the account.

3. A system, comprising:

at least one computing device; and

an authentication service executable in the at least one computing device, wherein when executed the authentication service causes the at least one computing device to at least:

in response to receiving from a first client a first authentication request for an account to log in to an application that specifies an incorrect security credential, determine that the authentication request is fraudulent based at least in part on at least one criterion;

record the incorrect security credential in a database of incorrect security credentials; and

in response to determining that a second authentication request for the account from a second client specifies the recorded incorrect security credential, provide the second client with access to a honeypot environment that is configured to mimic a successful login to the application via the account.

App. Br. 16–17 (Claims Appendix).

The Applied References

The Examiner relies on the following references as evidence of unpatentability of the claims on appeal:

MacKinnon	US 2004/0177276 A1	Sept. 9, 2004
Martin	US 2008/0018927 A1	Jan. 24, 2008
Zaslavsky	US 9,092,782 B1	July 28, 2015

The Examiner's Rejections

The Examiner made the following rejections of the claims on appeal:

Claims 1–8, 10, 11, and 13–19 stand rejected under 35 U.S.C. § 103 as being unpatentable over Martin and Zaslavsky. Final Act. 5–16.[2]

Claims 12, 20, and 21 stand rejected under 35 U.S.C. § 103 as being unpatentable over Martin, Zaslavsky, and MacKinnon. Final Act. 16–18.

ANALYSIS[3]

Appellant disputes the Examiner's finding that Martin and Zaslavsky render obvious, *inter alia*, independent claims 1 and 3. App. Br. 5–11; Reply Br. 4–11.

[2] The Final Action rejects claims 1–11 and 13–19 over Martin and Zaslavsky, however, Appellant previously had canceled claim 9, as noted in the Final Action. *See* Final Act. 2, 5. As such, we herein use corrected claim numbering for this rejection.

[3] Throughout this Decision, we have considered Appellant's Appeal Brief filed April 25, 2018 ("App. Br."); Appellant's Reply Brief filed August 20, 2018 ("Reply Br."); the Examiner's Answer mailed June 21, 2018 ("Ans."); the Final Office Action mailed October 31, 2017 ("Final Act."); and Appellant's Specification filed February 16, 2015 ("Spec.").

As to independent claim 1, Appellant argues Martin and Zaslavsky, alone or in combination, do not teach (a) "in response to determining that [a] login request specifies the incorrect password, determine whether the incorrect password corresponds to a known compromised password;" and (b) "in response to determining that the incorrect password corresponds to the known compromised password, provide the client with access to a honeypot environment that is configured to mimic a successful login via the account." App. Br. 6–8; Reply Br. 4–7.

Martin generally relates to surreptitiously and remotely monitoring usage of an electronic device for security purposes, and upon detection of a predetermined condition, switching the software environment of that device from a normal mode of operation to a honeypot mode of operation. *See* Martin ¶¶ 1, 19, 41. As found by the Examiner (Final Act. 5–6), Martin discloses "the pre-determined conditions 56 may include the input of ten or more incorrect password attempts by the device user." Martin ¶ 41. The Examiner finds this disclosure of "predetermined conditions" teaches determining whether a user login request specifies an incorrect password, and in response thereto, providing the user with access to a honeypot environment that is configured to mimic a successful login. Final Act. 5–6. But the Examiner finds Martin "fails to disclose the method of determining whether the incorrect password/credential corresponds to a known compromised credential," and turns to Zaslavsky. Final Act. 6.

Zaslavsky generally relates to "evaluating compromised credential records based on machine learning and pattern recognition methods." Zaslavsky 2:23–25. As found by the Examiner (Final Act. 6–7), Zaslavsky discloses that "by correlating various data elements known on each compromised record, records can be identified that are likely to be used for fraudulent activities, such as financial exploitation or theft of medical records." Zaslavsky 2:41–45. Zaslavsky also discloses "a ranked list of compromised credentials is generated that provides users with an improved ability to act upon the stolen credentials." Zaslavsky 2:46–60. The Examiner finds this disclosure in Zaslavsky teaches the claimed feature missing in Martin, namely, determining whether an incorrect password/credential corresponds to a known compromised credential. Final Act. 6.

Section 103 forbids issuance of a patent when "the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains." 35 U.S.C. § 103; *see Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 13 (1966). To support the legal conclusion of obviousness, "there must be some articulated reasoning with some rational underpinning" for combining elements in the manner claimed. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

Appellant argues that although Martin discloses "conditions under which the device 10 switches from normal operating mode to honeypot operating mode" (Martin ¶ 41), "*Martin* fails to show or suggest that 'determining that the incorrect password corresponds to the known compromised password' would be such a condition." App. Br. 8; Reply Br. 7. Appellant also argues "*Zaslavsky* fails to cure this deficiency because (1) . . . *Zaslavsky* does not show or suggest this particular condition relating to assessing incorrect passwords, and (2) Zaslavsky does not appear to discuss honeypot environments at all." App. Br. 8; Reply Br. 6–7. Appellant further argues that, in claim 1, "the client is provided with access to a honeypot environment '*in response to* determining that the incorrect password corresponds to the known compromised password,' not simply in response to an incorrect password being provided." Reply Br. 4 (emphasis added). Appellant submits "there is no logical connection between the compromised credential evaluation of *Zaslavsky* and the multiple incorrect password attempts of *Martin*." Reply Br. 6.

We agree with Appellant that the Examiner has not sufficiently shown that Martin and Zaslavsky, alone or in combination, teach the disputed limitations in independent claim 1. Claim 1 requires a specific sequence of steps that, plainly stated, (1) determine incorrect passwords; (2) determine whether the incorrect passwords correspond to known compromised passwords; and (3) provide a honeypot environment when such incorrect passwords are compromised passwords, with each step being performed "in response to" the prior step. *See* Claim 1. Our reviewing court has stated the phrase "'[i]n response to' connotes that the second event occur in reaction to the first event." *Am. Calcar, Inc. v. Am. Honda Motor Co.*, 651 F.3d 1318, 1340 (Fed. Cir. 2011). Although Martin teaches determining incorrect passwords (step (1) above) as a condition for switching from a normal to a honeypot operating mode (the outcome of step (3) above), and Zaslavsky teaches evaluating risk associated with known compromised passwords (an aspect of step (2) above), we find the Examiner has not provided sufficient evidence or persuasive technical reasoning that Martin and Zaslavsky teach ordered steps (2) and (3) above, namely, determining whether an incorrect password corresponds to known compromised passwords, and if so, providing a client with access to a honeypot environment configured to mimic a successful login.

For the reasons discussed *supra*, we do not sustain the Examiner's rejection under 35 U.S.C. § 103 of independent claim 1. Additionally, we do not sustain the Examiner's rejections of claims 2 and 21, which depend therefrom.

As to independent claim 3, Appellant argues Martin and Zaslavsky, alone or in combination, do not teach (a) "record[ing] [an] incorrect security credential in a database of incorrect security credentials;" and (b) "in response to determining that a second authentication request for the account from a second client specifies the recorded incorrect security credential, provide the second client with access to a honeypot environment that is configured to mimic a successful login to the application via the account." App. Br. 8–11; Reply Br. 7–11.

The Examiner turns to Zaslavsky's disclosure of "collecting data regarding previously compromised credentials that were used to commit an unauthorized activity," and finds this teaches recording incorrect security credentials in a database of incorrect security credentials. Ans. 19 (citing Zaslavsky 1:43–52) (emphasis omitted); Final Act. 8–9. Appellant responds that "[a]lthough *Zaslavsky* discusses 'collecting data regarding previously compromised credentials,' . . . this is different from 'record[ing] the incorrect security credential in a database of incorrect security credentials,'" and submits that "[a] previously compromised credential is not necessarily an incorrect security credential," rather, "in order to be compromised, the previously compromised credential had to be correct at some time." App.

Br. 9–10. The Examiner also finds Martin's disclosure of two operating modes, normal and honeypot, teaches the claimed first client and second client, and Martin's disclosure of "predetermined conditions" (such as an incorrect password) teaches providing the second client with access to the honeypot environment. Final Act. 7–9; Ans. 19–21. Appellant responds that although Martin discloses certain "predetermined conditions," "*Martin* fails to show or suggest that 'determining that a second authentication request for the account from a second client specifies the recorded incorrect security credential' would be such a condition." App. Br. 10–11. Appellant also argues that claim 3 requires "two separate clients," and "*Martin* fails to show or suggest providing a client with access to a honeypot environment when that client specifies the same incorrect security credential that a different client had provided previously." App. Br. 11.

We again agree with Appellant that the Examiner has not sufficiently shown that Martin and Zaslavsky, alone or in combination, teach the disputed limitations in independent claim 3. Claim 3 requires a specific sequence of steps that, plainly stated, (1) receive an incorrect security credential from a first client; (2) record that incorrect security credential in a database; and (3) *in response to* receiving from a second client a recorded incorrect security credential, provide the second client with access to a honeypot environment. *See* Claim 3. Although Martin teaches determining incorrect passwords (step (1) above) as a condition for switching from a normal to a honeypot operating mode (the outcome of step (3) above), and Zaslavsky teaches collecting and evaluating data regarding previously compromised credentials/passwords (an aspect of "recording" data in step (2) above), we find the Examiner has not provided sufficient evidence or persuasive technical reasoning that Martin and Zaslavsky teach ordered steps (2) and (3) above, namely, recording an incorrect security credential from a *first* client, and subsequently providing a *second* client that uses recorded incorrect security credentials with access to a honeypot environment.

For the reasons discussed *supra*, we do not sustain the Examiner's rejection under 35 U.S.C. § 103 of independent claim 3. Additionally, we do not sustain the Examiner's rejections of claims 4–8 and 10–13, which depend therefrom. For similar reasons, we do not sustain the Examiner's rejections of independent claim 14, which recites commensurate limitations with independent claim 3, and claims 15–20, which depend therefrom.

CONCLUSION

Claims Rejected	**Basis**	**Affirmed**	**Reversed**
1–8, 10, 11, and 13–19	§ 103 Martin and Zaslavsky		1–8, 10, 11, and 13–19
12, 20, and 21	§ 103 Martin, Zaslavsky, and MacKinnon		12, 20, and 21
Overall Outcome			1–8 and 10–21

REVERSED