

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

F5, INC.,
Petitioner,

v.

SUNSTONE INFORMATION DEFENSE, INC.,
Patent Owner.

IPR2022-00484
Patent 10,958,682 B2

Before JAMESON LEE, JON M. JURGOVAN, and AMBER L. HAGY,
Administrative Patent Judges.

JURGOVAN, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

F5, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1–6, 8, 12, 16, 21–25, 27, 28, 32, and 36¹ (“challenged claims”) of U.S. Patent No. 10,958,682 B2 (Ex. 1001, “the ’682 patent”). Paper 2 (“Pet.”). Sunstone Information Defense, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 9 (“Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review, under 35 U.S.C. § 314 and 37 C.F.R. § 42.4. An *inter partes* review may not be instituted unless it is determined 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.” 35 U.S.C. § 314(a) (2018); *see also* 37 C.F.R. § 42.4(a) (2021) (“The Board institutes the trial on behalf of the Director.”). The “reasonable likelihood” standard is “a higher standard than mere notice pleading,” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

For the reasons provided below and based on the record before us, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing the unpatentability of at least one challenged claim. Accordingly, we do not institute an *inter partes* review on any claim of the ’682 patent on any asserted ground of unpatentability.

¹ Claims 12 and 16 were omitted from Petitioner’s listing of challenged claims but they are discussed in the Petition. Pet. 61–63.

B. Real Parties in Interest

Petitioner identifies itself and Capital One Financial Corporation as real parties in interest. Pet. 2. Patent Owner identifies itself as the only real party in interest. Paper 5, 1.

C. Related Proceedings

Petitioner and Patent Owner each identify the following related litigations involving the '682 patent: *Sunstone Information Defense, Inc. v. F5 Networks, Inc. and Capital One Financial Corporation*, Civil Action No. 3:21-CV-09529 (N.D. Ca.); and *Sunstone Information Defense, Inc. v. International Business Machines Corporation*, Civil Action No. 6:20-CV-01033-ADA (W.D. Tex.). Pet. 2; Paper 5, 1.

The following *inter partes* review proceedings involve patents related to the '682 patent: IPR2022-00482 (U.S. Patent No. 9,122,870 B2); IPR2022-00483 (U.S. Patent No. 10,230,759 B2).

D. The '682 Patent (Ex. 1001)

The '682 patent discloses a system for validating communication between a server and a client device by predicting a response of the client device to the server in order to identify malicious applications that interfere with such communications. Ex. 1001, 3:66–4:4. Malicious applications create noise to alter, access, or hijack data and/or content being communicated across a client-server connection. *Id.* at 4:39–44. For instance, by using noise, viruses and other types of malicious applications can direct a client device (e.g., a receiver) to perform actions that a server (e.g., a sender) did not originally intend. *Id.* at 2:37–40.

The '682 patent purports to solve these problems by a system for “detecting malicious applications through estimated, predicted, or

anticipated responses from a client device.” *Id.* at 5:25–29. During a client-server connection, a server provides hard information and soft information to the client device. *Id.* at 5:32–34. The hard information includes data, text, and other information that is important for carrying out a transaction with a client, and the soft information specifies how the hard information is to be rendered and displayed by the client device. *Id.* at 5:34–38. The ’682 patent discloses detecting malicious applications by varying the soft information describing how hard information is to be displayed by a client device. *Id.* at 5:29–32.

Variations in soft information form a best guess (e.g., a prediction or estimation) as to how hard information is displayed by a client device. *Id.* at 5:49–52. The system then compares an actual response from the client device to the best guess response. *Id.* at 5:52–54. If the actual response does not match or is not close enough to the predicted response, then the system concludes a malicious application is affecting the communication between server and client device. *Id.* at 5:54–60. As a result of this detection, the system implements failsafe procedures to reduce the effects of the malicious application. *Id.* at 5:60–63.

Figure 7 of the ’682 patent is reproduced below:

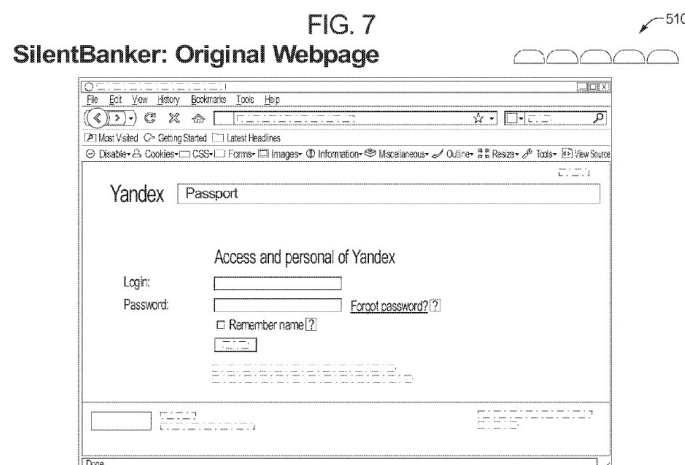


Figure 7 illustrates an image of datagram 510 including the server's request for a username and password. Ex. 1001, 19:32–33. The server uses datagram 510 to predict how the client device will process, render, and display datagram 502. *Id.* at 19:34–36. A malicious application, however, may use channel noise to alter the transmitted soft and/or hard information, for example, to add a security question not sent by the server and move the submit button to make room for the added security question. *Id.* at 19:47–54.

Figure 8 of the '682 patent is reproduced below:

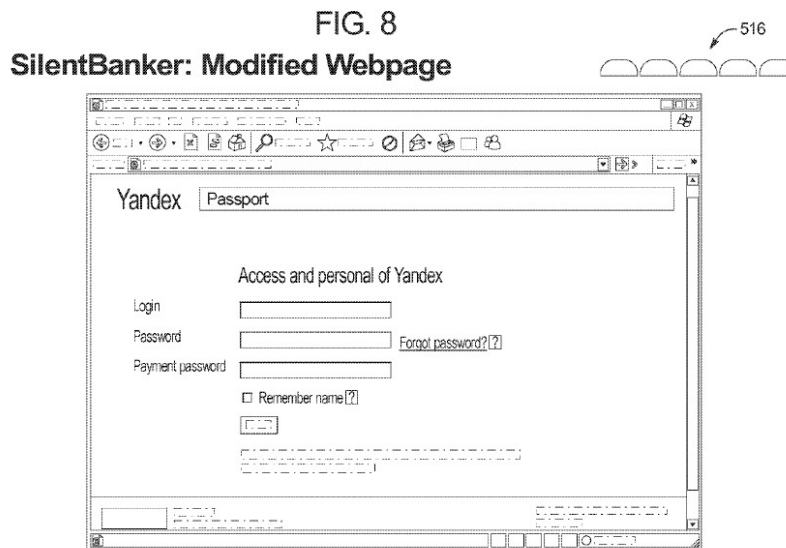


Figure 8 shows a rendered datagram as displayed on the client device as altered by the malicious application, which shows an added security question and displacement of the submit button to a different location as a result of the addition of the security question. *Id.* at 19:48–52. The security question appears to be genuine to a user of the client device, even though it is not. *Id.* at 19:52–54. The malicious application then removes the answer to the security question but leaves alone the soft information such as the location of the mouse click by the user. *Id.* at 19:57–60.

Figure 9 of the '682 patent is reproduced below:

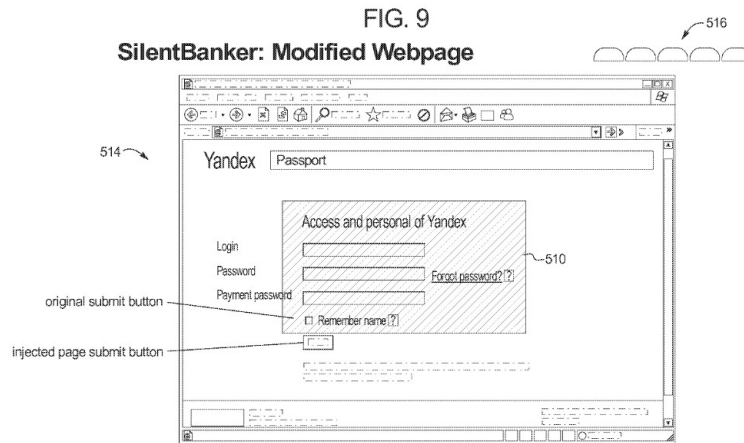


Figure 9 illustrates a comparison made by a security processor to determine if a malicious application is affecting communication between the server and the client device. *Id.* at 20:8–12. The prediction datagram is superimposed on the actual datagram received from the client device. *Id.* at 20:16–18. The '682 patent explains:

[B]y comparing the prediction position of the “submit” button with the directly reported position, security processor 112 detects whether an error has occurred during communication session 300. Here, security processor 112 detects that the datagram 514 does not align with the datagram 510, and accordingly determines that [a] malicious application 304 is affecting communications.

Id. at 20:35–42.

E. Illustrative Claim

Claim 1 is independent and reproduced below:²

1. A method comprising:
 - [1.a] selecting, via a processor, transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device;
 - [1.b] selecting, via the processor, presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed;
 - [1.c] transmitting, via the processor, at least one message including the presentation and transactional information from the server to the client device;
 - [1.d] determining, via the processor, a prediction of a response message from the client device based on i) the selected transactional information, ii) how the client device is configured to render the transactional information specified by the presentation information, and iii) expected response information associated with the transactional information that is expected to be provided by a user of the client device;
 - [1.e] receiving, in the processor, the response message from the client device; and
 - [1.f] responsive to information in the response message not matching the prediction, providing an indication there is a malicious application affecting communications between the server and the client device,
 - [1.g] wherein the prediction is further determined by the processor based at least in part by estimating at least one location of at least one rendered feature or function as displayed by the client device,

² We added the bracketed captions for the claim elements for ease of reference and understanding.

[1.h] wherein the presentation information includes at least one of protocol information, formatting information, positional information, rendering information, style information, transmission encoding information, information describing how different layers of a style sheet are to be rendered by the client device, or information changing a definition of a function in a code library at the client device, and

[1.i] wherein the transactional information includes at least one of text, data, pictorial information, image information, information requested by the server to perform a service for the client device, authentication information, refinement information on a type of service requested by the client device, financial information, or data management information.

Ex. 1001, 29:51–30:30.

F. Evidence Relied on by Petitioner

Petitioner relies on the following evidence:³

References		Date	Exhibit
Ozzie	U.S. Pub. App. 2010/0100725 A1	Published Apr. 22, 2010	Ex. 1003 ⁴
Chen	U.S. Pub. App. 2008/0134338 A1	Published June 5, 2008	Ex. 1002 ⁵

³ The '682 patent issued from Application 16/298,537, filed Mar. 11, 2019, which is a continuation of Application 14/841,083, filed August 31, 2015, now Patent 10,230,759, which is a continuation of 13/623,556, filed Sep. 20, 2012, now Pat. 9,122,870. Ex. 1001, codes (21), (22), (63). The '682 patent claims priority to Provisional Application 61/557,733, filed Nov. 9, 2011, and Provisional Application 61/537,380, filed Sep. 21, 2011. *Id.* at code (60).

⁴ Petitioner contends that Ozzie is prior art under pre-AIA 35 U.S.C. § 102(e). Pet. 11.

⁵ Petitioner contends that Chen is prior art under pre-AIA 35 U.S.C. § 102(b). Pet. 11.

References		Date	Exhibit
Frantz	U.S. Pat. 8,756,684 B2	Issued June 17, 2014	Ex. 1004 ⁶
Boodaei	U.S. Pub. App. 2008/0222736 A1	Published Sep. 11, 2008	Ex. 1005 ⁷

Pet. 11.

Petitioner also relies on the Declaration of Markus Jakobsson, Ph.D. (Ex. 1006).

G. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–6, 8, 12, 16, 21–25, 27, 28, 32, and 36 of the '682 patent on the following grounds:

Claims Challenged	35 U.S.C. § ⁴	Reference(s)/Basis
1–3, 6, 8	103	Ozzie, Chen
4	103	Ozzie, Chen, Frantz
5, 12, 16, 21–25, 27, 28, 32, 36 ⁸	103	Ozzie, Chen, Boodaei

Pet. 11.

⁶ Petitioner contends that Frantz is prior art under pre-AIA 35 U.S.C. § 102(e). Pet. 11.

⁷ Petitioner contends that Boodaei is prior art under pre-AIA 35 U.S.C. § 102(b). Pet. 11.

⁸ See footnote 1.

II. ANALYSIS

A. *Level of Ordinary Skill in the Art*

Petitioner contends that a person of ordinary skill in the art at the time of the alleged invention “will have had either a master’s degree in computer science with at least two-years’ experience developing technology for detecting malware affecting internet browsers or a bachelor’s degree with four years of said experience.” Pet. 12 (citing Ex. 1006 ¶ 42). Patent Owner has not proposed a differently stated level of ordinary skill in the art. *See generally* Prelim. Resp. Nor has Patent Owner opposed Petitioner’s statement of the level of ordinary skill.

Petitioner’s assertion is supported by the testimony of Dr. Jakobsson. Ex. 1006 ¶ 42. Petitioner’s assertion also appears consistent with the content of the applied prior art references. *Okajima v. Bourdeau*, 261 F.3d 1350, 1354–55 (Fed. Cir. 2001) (the applied prior art may reflect an appropriate level of skill). We adopt Petitioner’s statement of the level of ordinary skill in the art, but delete the modifier “at least” to avoid vagueness and to keep the level of ordinary skill from extending into a level above “ordinary.”

B. *Claim Construction*

We use the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b). The claim construction standard set forth in *Phillips v. AWH Corporation*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), is applicable.

Claim terms are generally given their ordinary and customary meaning as would be understood by one with ordinary skill in the art in the context of the specification, the prosecution history, other claims, and even extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Phillips*, 415 F.3d at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

The specification may reveal a special definition given to a claim term by the patentee, or the specification or prosecution history may reveal an intentional disclaimer or disavowal of claim scope by the inventor. *Id.* at 1316. If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). The disavowal, if any, can be effectuated by language in the specification or the prosecution history. *Poly-America, L.P. v. API Indus., Inc.*, 839 F.3d 1131, 1136 (Fed. Cir. 2016).

Only those claim terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

Neither Petitioner nor Patent Owner has proposed a construction for any claim term. Patent Owner states that no claim construction is necessary to determine whether review should be instituted. Prelim. Resp. 11. We determine that no express claim construction is necessary for this Decision.

C. Alleged Obviousness of Claims 1–3, 6, and 8 over Ozzie and Chen

1. Legal Principles on Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations, including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). “[T]here must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *Kahn*, 441 F.3d at 988.

2. Overview of Ozzie (Ex. 1003)

Ozzie describes a multi-factor authentication service that is used to verify that the entity communicating with a server is human and not an automated Internet bot. Ex. 1003 ¶¶ 22, 24. The authentication service provides an authentication-test message that asks a user for a specific response to authenticate the user to the host server. *Id.* ¶ 27. In one embodiment, a website displays an image of distorted letters and numbers,

e.g., a CAPTCHA image, and asks the user to input the text from the image in a response box. *Id.* ¶ 22. While a human user may be able to decipher the text in the image, a computer may not be able to effectively determine the text. *Id.*

The authentication-test message may be randomly generated by the user authentication service and displayed on a host website's webpage. *Id.* ¶ 27. Alternatively, the user authentication service can send an authentication-request message to the user's mobile device. *Id.* ¶ 28. The authentication-request message also may request that the user respond to the message using the mobile device. *Id.*

The host website can create a cross-domain inline frame (Iframe), which is controlled by the user authentication service. In this way, the user authentication service can provide notifications, messages, and codes to a website user using the Iframe. *Id.* ¶ 35. In this Iframe configuration, the user authentication service provides the remaining elements of the user authentication remotely, for example, with the host website doing nothing else. *Id.* ¶ 35. Figure 6 of Ozzie is reproduced below:

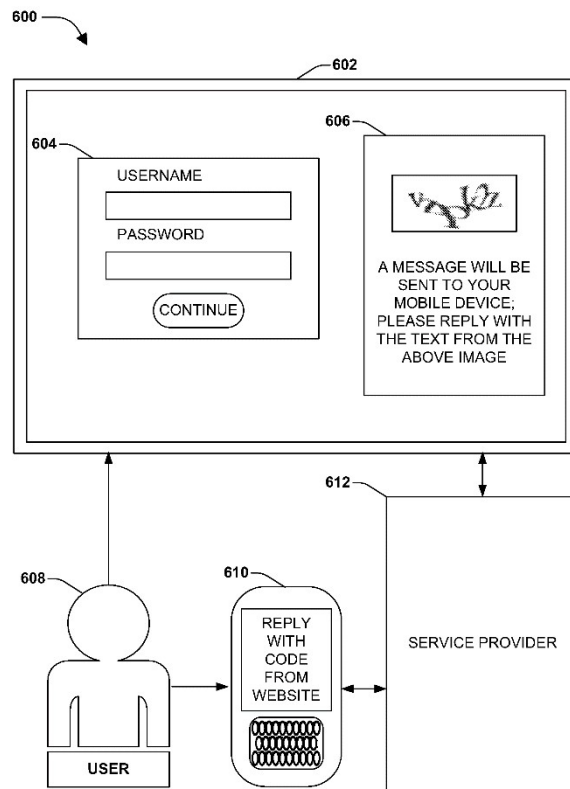


FIG. 6

Figure 6 illustrates an example of multi-factor user authentication. *Id.* ¶ 42. Browser page 602 comprises first authentication factor 604 in the form of a user log in, using a username and password. *Id.* When user 608 initiates authentication by entering the username and password into login box 604, user authentication service 612 automatically detects user authentication using API (Application Programming Interface) code, and initiates user interface 606 (UI) in a cross-domain Iframe on browser page 602. *Id.* In this example, the UI can contain an image of distorted text (e.g., a CAPTCHA image), and a status message telling the user that a message will be sent to user's mobile device 610, along with instructions on how to proceed. *Id.*

3. *Overview of Chen (Ex. 1002)*

Chen provides that graphical user interface (GUI) logic flaws are a category of software vulnerabilities that result from logic flaws in GUI implementation, and that it discloses a way to uncover such logic flaws in the software by using a systematic reasoning approach. Ex. 1002, code (57). The described method includes three major steps: (1) mapping a visual invariant to a program invariant; (2) formally modeling the program logic, user actions and execution context and systematically exploring the possibilities of violations of the program invariant; and (3) finding real spoofing attacks based on the exploration. *Id.*

Chen provides that graphical interfaces such as those of web browsers have vulnerabilities in the form of visual spoofing, such as address bar spoofing and status bar spoofing which can lure even experienced users to perform unintended actions. *Id.* ¶ 1. The combination of email status bar spoofing and browser status bar spoofing gives an “authentic” browsing experience to a faked web page. *Id.* Chen recognizes that visual spoofing flaws have been discovered in various web browser programs and that they can be “due to GUI logic flaws” in the browser program. *Id.* ¶ 4.

Chen provides a methodology to uncover logic flaws in the graphical user interface of web browsers. *Id.* ¶ 5. The methodology maps a visual invariant to a program invariant. Chen states: “a visual invariant of the status bar may be that if the user sees the address ‘foo.com’ on a status bar before a mouse click, then it is expected that ‘click’ action navigates to the page ‘foo.com.’ Therefore, a map is performed based on a visual invariant to a program invariant in order to supply formal reasoning.” *Id.* ¶ 26. The visual invariant here is that “the web site that a user navigates to must be the same as that indicated on the status bar.” *Id.* ¶ 28. A program invariant “is a

Boolean condition about user state and software state.” *Id.* ¶ 6. Specific examples of program invariants include: “the impossibility of buffer overrun, guaranteed mutual exclusion in an algorithm, deadlock freedom, and secrecy in cryptographic protocol.” *Id.* ¶ 26.

The mapping of visual invariant to program invariant is done based on an in-depth understanding of the source code of the browser’s software. *Id.* ¶ 6. An in-depth understanding of the browser’s logic or logic problems for mouse handling and page loading allows the ability to derive the program invariant. *Id.* ¶ 27. The source code of the browser software is studied for that purpose. *Id.*

Figure 1 of Chen is reproduced below:

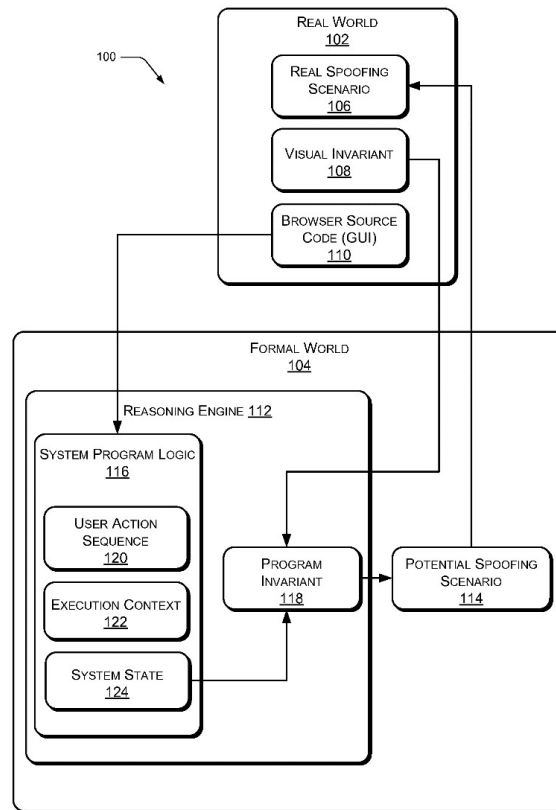


Fig. 1

Figure 1 illustrates system 100 which identifies GUI logic flaws in browser software. *Id.* ¶ 29. System 100 includes real world subsystem 102 and formal world subsystem 104. *Id.* Real world subsystem 102 includes one or more real spoofing scenarios 106, one or more visual invariants 108, and browser (GUI) source code 110. *Id.* Formal world subsystem 104 includes reasoning engine 112 and one or more potential spoofing scenarios 114. *Id.* Reasoning engine 112 further includes system program logic 116 and one or more program invariants 118. *Id.* System program logic 116 includes a user's action sequence 120, execution context 122, and system state 124. *Id.*

Chen explains:

The visual invariant 108 and source code 110 may be first mapped from the real world subsystem 102 to the formal world subsystem 104 by formally specifying them on the reasoning engine 112. The user action sequence 120, the execution context 122, and the system state 124 may also be formally specified. The reasoning engine 112 then performs mechanical reasoning to check whether the user action sequence 120 applied on a system running the system program logic 116 on the execution context 122 violates the program invariant 118. Each discovered violation is output as a potential spoofing scenario 114, which consists of the user action sequence 120, the execution context 122 and the system state 124 or inference steps for the particular real world spoofing scenario 106. Mapping back to the particular real world spoofing scenario 106 may include constructing a real web page that sets up the execution context 122 which lures a user to perform the action sequence 120.

Id. ¶ 30. Chen further explains that the reasoning applied is based on canonicalization which is a common form of abstraction used in formal reasoning practice to handle a complex problem space. *Id.* ¶ 52. Since any instance in an original problem space may only trivially differ from its canonical form, the canonical space is explored to find “representative”

instances. *Id.* For example, a set of user action sequences is mapped to a single canonical user action sequence, e.g., user action sequence 120. *Id.*

Through formal reasoning, Chen finds all execution paths that start with an initial state and finish in a bad state. *Id.* ¶ 104. A spoofing state is “not goodstate” and can be one where there is a mismatch in the URL on the address bar and the URL of the content that is displayed on the screen. *Id.*

¶ 100. Figure 11 of Chen is reproduced below:

1100



	Number 1102	Location 1104	Condition 1106
1108(1)	1	FireNavigationComplete	GetHTMLWinUrl() = NULL
1108(2)	2	FireNavigationComplete	GetPFD(bstrUrl)=NULL
1108(3)	3	FireNavigationComplete	ActivatedView = true
1108(4)	4	NavigationComplete	DontFireEvents = true
1108(5)	5	NavigationComplete	DocInPP = true
1108(6)	6	NavigationComplete	ViewWOC = true
1108(7)	7	NavigationComplete	ObjectTG = true
1108(8)	8	NavigationComplete	CreateDFU = true
1108(9)	9	SetAddressBar	CurrentUrl = NULL
1108(10)	10	SetClientSite	QIClassID()= OK
1108(11)	11	LoadHistory	HTMLDoc = NULL
1108(12)	12	CreateMarkup	NewMarkup = NULL
1108(13)	13	SetInteractive	pPWindowPrxy=NULL
1108(14)	14	SetInteractive	IsPassivating = true/IsPassivated
1108(15)	15	SetInteractive	HtmCtx() = NULL ¹⁷
1108(16)	16	SetInteractive	HtmCtx()->BindResult = OK
1108(17)	17	EnsureView	IsActive() = false
1108(18)	18	RenderView	RSFC = NULL

Figure 11

Figure 11 is a table including 18 entries representing resulting uncovered states and conditions that suggest a potential spoofing scenario. *Id.* ¶¶ 20, 105. Table 1100 provides a roadmap for further systematic investigation by use of a debugger. *Id.* ¶ 105. For instance, it can be verified whether “when each of the conditions 1106 is manually set to true in the corresponding location using a debugger, the real browser executable will be forced to take an execution path leading to a stable bad state.” *Id.*

¶ 106. The further systematic investigation focuses on conditions 1106. *Id.*

4. *Independent Claim 1*

Claim 1 begins with this preamble: “A method comprising.” Ex. 1001, 29:51. Petitioner asserts that Ozzie discloses a method for providing a remote computer user authentication service. Pet. 17 (citing Ex. 1003 ¶ 23). Patent Owner does not dispute that Ozzie describes such a method. *See generally* Prelim. Resp. Petitioner has sufficiently accounted for the preamble recitation.

Claim 1 recites limitation [1.a] as follows: “selecting, via a processor, transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device.” Ex. 1001, 29:52–54. Petitioner asserts that Ozzie discloses selecting a test message which is the claimed transactional information to send from a host’s webpage to a user in response to a user authentication request. Pet. 18 (citing Ex. 1003 ¶ 26). Petitioner further asserts that the test message is transactional information as it may involve a username and password to authenticate a user. *Id.* (citing Ex. 1003 ¶ 42). Patent Owner does not dispute that Ozzie describes limitation 1(a). We are sufficiently persuaded by Petitioner that Ozzie discloses limitation [1.a].

Claim 1 recites limitation [1.b] as follows: “selecting, via the processor, presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed.” Ex. 1001, 29:55–59. Petitioner asserts that Ozzie’s test message, i.e., the transactional information, is implemented in a user interface, is sent in the form of a user interface, and is displayed according to selected presentation information in the user interface. Pet. 19–20. Petitioner further explains that Ozzie teaches different interfaces which are arranged according to different

selections of presentation information, citing Figures 1, 2, and 6 of Ozzie.
Id. at 20. According to Petitioner, these disclosures satisfy claim limitation [1.b]. Figures 1, 2, and 6 of Ozzie are reproduced below:

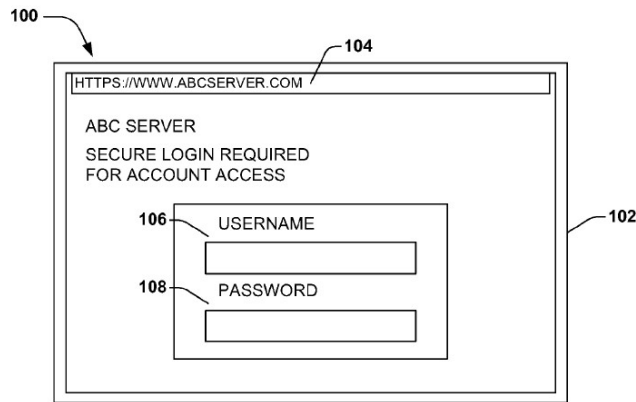


FIG. 1

Figure 1 shows a block diagram of an exemplary embodiment of Ozzie implementing one factor authentication. Ex. 1003 ¶ 10.

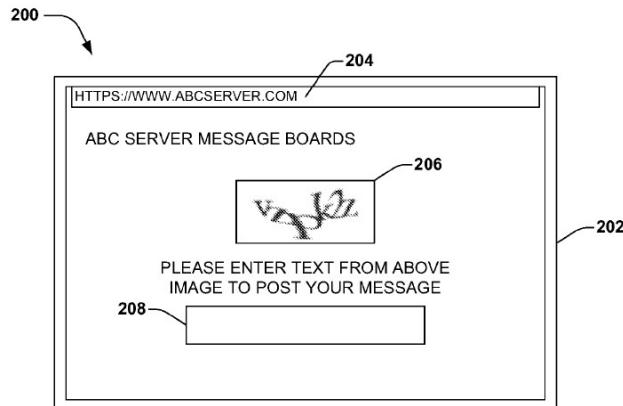


FIG. 2

Figure 2 is an illustration of challenge response test posed by a website for an appropriate user response. *Id.* ¶ 22.

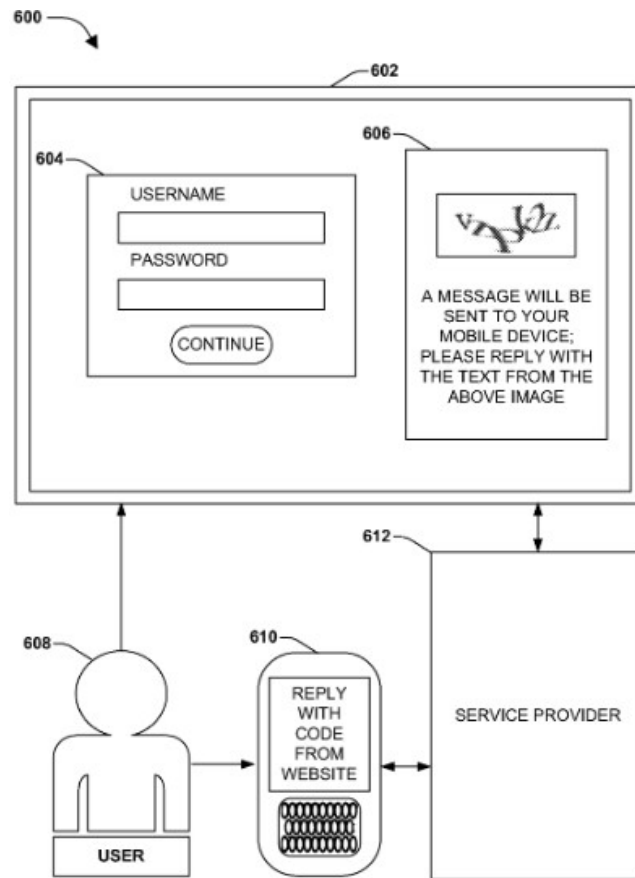


FIG. 6

Figure 6 shows a block diagram of an exemplary embodiment of Ozzie implementing multi-factor authentication. Ex. 1003 ¶ 15.

Petitioner's assertions are supported by the cited evidence. Patent Owner does not dispute that Ozzie describes limitation [1.b]. We find sufficient Petitioner's showing that Ozzie discloses limitation [1.b].

Claim 1 recites limitation [1.c] as follows: "transmitting, via the processor, at least one message including the presentation and transactional information from the server to the client device." Ex. 1001, 29:60–62. Petitioner asserts that Ozzie discloses initiating a user authentication interface in an Iframe of a host website displayed on a user's browser. Pet. 23. Petitioner explains that Ozzie transmits the user interface by initiating

the UI in the Iframe on a webpage that a user is accessing. *Id.* (citing Ex. 1003 ¶ 38). Petitioner explains that Ozzie’s test message is transactional information, that the test message is arranged into a selected user interface according to presentation information, and that the selected user interface is transmitted. *Id.* On this basis, Petitioner asserts that Ozzie transmits a UI comprising transactional and presentation information. *Id.* at 22–23.

Petitioner’s assertions are supported by the cited evidence. Patent Owner does not present arguments to the contrary. Petitioner has shown sufficiently that Ozzie discloses limitation [1.c].

Claim 1 recites limitation [1.d] as follows: “determining a prediction of a response message from the client device based on i) the selected transactional information, ii) how the client device is configured to render the transactional information specified by the presentation information, and iii) predicted response information associated with the transactional information that is expected to be provided by a user of the client device.” Ex. 1001, 29:63–30:3.

Petitioner’s accounting of limitation [1.d] has multiple deficiencies, as we discuss below.

First, Petitioner splits limitation [1.d] into two parts, and applies Chen’s teachings to meet the first part, i.e., subsections (i) and (ii) of limitation [1.d] (Pet. 23–28), and Ozzie’s teachings to meet the second part, i.e., subsection (iii) of limitation [1.d] (Pet. 28). There is no explanation by Petitioner of how the combination of Ozzie and Chen results in satisfaction of all three subsections (i), (ii), and (iii) of limitation [1.d] at the same time in a single embodiment. On the record presented by Petitioner, at most only subsections (i) and (ii) of limitation [1.d] are met, or subsection (iii) is met,

but not all three subsections (i), (ii), and (iii) at once as is required by claim 1.

One seeking to establish obviousness based on more than one reference must articulate sufficient reasoning with rational underpinning to combine teachings. *See KSR Int'l*, 550 U.S. at 418. Petitioner has not presented reasoning with rational underpinning to support satisfaction of all three subsections (i), (ii), and (iii) together in a single embodiment. The carving up of limitation [1.d] into two parts and satisfying the two parts separately by relying on different references, one for each part, fails to treat limitation [1.d] as a whole and is improper.

Second, Petitioner identifies Chen's user actions as the claimed response message. Pet. 21. But Chen's "user actions" are canonical, i.e., theoretical possibility, and used only for formal reasoning analysis, as discussed above in Section II.C.3. They have not been shown by Petitioner to be actual responses in a real communication between a server and a user. Chen's user action or user actions do not constitute a response message. Further, Petitioner has not shown how Chen's canonical user action corresponds in kind to any actual response message in Ozzie. Petitioner's application of Chen in Ozzie to make a real response message from Chen's canonical user actions reflects application of inappropriate hindsight reasoning and is not reasonably suggested by the applied prior art.

Third, Petitioner identifies Chen's program invariant as the claimed prediction of a response message. Pet. 21. But Chen's "program invariant," as discussed above in Section II.C.3, is not any expected or anticipated information that is returned to any server from a client. It is not the prediction of any response message. Further, Petitioner has not shown how Chen's program invariant corresponds in kind to any prediction of an actual

response message in Ozzie. Petitioner's application of Chen in Ozzie to make a prediction of a response message from Chen's program invariant reflects application of inappropriate hindsight reasoning and is not reasonably suggested by the applied prior art.

Fourth, even assuming that Chen's user action or user actions are a response message and also that Chen's program invariant is a prediction of a response message, there is no correspondence in kind between the two. Indeed, the alleged prediction, i.e., program invariant, is not a set of user actions. Petitioner points to no disclosure in Chen that the program invariant in Chen conveys what user action or user actions would, or should, be taken. It is implicit in the claim that the response message and the prediction of the response message must correspond in kind, as limitation [1.f] requires a comparison between the response message and the prediction of a response message to determine if there is a match.

Fifth, Chen's system, as discussed above in Section II.C.3, requires further systematic investigation with use of a debugger even after the reasoning engine identifies violations of a program invariant which potentially may be a spoofing scenario. Ex. 1002 ¶¶ 104–106. Such an approach is unsuitable for incorporation into Ozzie's system which requires immediate authentication of user identity. Petitioner points to no disclosure in Chen that indicates that Chen's system is useful for uncovering spoofing in action. Rather, Chen specifically describes that it discloses a way to uncover logic flaws in software. Ex. 1002, code (57). Chen is concerned with prevention of spoofing, and Petitioner has not sufficiently shown that the ordinarily skilled artisan would have understood Chen's teachings to apply to the actual apprehension of spoofing in progress, usable in the authentication procedure of Ozzie.

For the foregoing reasons, Petitioner has not sufficiently shown that the combined teachings of Ozzie and Chen disclose limitation [1.d]. Petitioner has not shown a reasonable likelihood that it would prevail in establishing obviousness of claim 1 over Ozzie and Chen.

5. *Claims 2, 3, 6, and 8*

Claims 2 and 3 depend from claim 1 and incorporate all of its limitations. Claims 6 and 8 are independent claims with the same limitations discussed with respect to claim 1. For the same reasons stated for claim 1, Petitioner has not shown a reasonable likelihood to prevail in demonstrating any of these claims unpatentable as obvious over the combination of Ozzie and Chen.

6. *Conclusion*

Petitioner has not shown a reasonable likelihood that it would prevail in establishing obviousness of claims 1–3, 6, and 8 of the '682 patent over the combination of Ozzie and Chen.

D. *Alleged Obviousness of Claim 4 over Ozzie, Chen, and Frantz*

Claim 4 depends from claim 1 and includes all of the limitations of that claim. With regard to independent claim 4, Frantz has been applied as disclosing the further actions of restricting access to a client device or transmitting an alert and entering a safe operations mode upon determining that the received response message does not match the expected response message from the client device. Pet. 51–53. Petitioner has not shown that Frantz covers the deficiencies of Ozzie and Chen as noted above for claim 1. Consequently, Petitioner has not shown a reasonable likelihood that claim 4 of the '682 patent is unpatentable over the combination of Ozzie, Chen and Frantz.

E. Alleged Obviousness of Claims 5, 12, 16, 21–25, 27, 28, 32, and 36 over Ozzie, Chen, and Boodaei

Claims 12, 16, 21, 25, 28, 32, and 36 are independent claims incorporating the limitations [1.a] to [1.d] of claim 1 discussed previously. Petitioner relies on Boodaei to teach or suggest equivalent limitations to limitation [1.g]. Pet. 59. Petitioner does not rely on Boodaei to disclose limitations in independent claims 12, 16, 21, 25, 32, and 36 that are equivalent to limitation [1.d] discussed above. Consequently, for the reasons previously explained concerning limitation [1.d], the Petition does not show a reasonable likelihood to prevail in demonstrating unpatentability of independent claims 12, 16, 21, 25, 32, and 36 as obvious over the combination of Ozzie, Chen, and Boodaei.

Claims 5, 23–24, and 27 depend from respectively independent claims 1, 21, and 27, and thus incorporate all of their limitations. For the reasons explained, the Petition does not demonstrate a reasonable likelihood to prevail in showing that these dependent claims of the '682 patent are unpatentable as obvious over the combination of Ozzie, Chen, and Boodaei.

III. CONCLUSION

We determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in establishing that at least one of challenged claims 1–6, 8, 12, 16, 21–25, 27, 28, 32, and 36 of the '682 patent is unpatentable.

IV. ORDER

It is

ORDERED that the Petition is *denied*, and that no trial is instituted.

IPR2022-00484
Patent 10,958,682 B2

For Petitioner:

Brent P. Ray
D. Shane Brun
KING & SPALDING LLP
bray@kslaw.com
sbrun@kslaw.com

For Patent Owner:

Michael D. Saunders
Bryan D. Atkinson
DICKINSON WRIGHT PLLC
msaunders@dickinson-wright.com
batkinson@dickinson-wright.com