



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.
12/968,095	12/14/2010	Yin Wei	1217-038US01	1755
72689	7590	10/28/2016	EXAMINER	
SHUMAKER & SIEFFERT, P.A 1625 RADIO DRIVE , SUITE 100 WOODBURY, MN 55125			GUIRGUIS, MICHAEL M	
			ART UNIT	PAPER NUMBER
			2498	
			NOTIFICATION DATE	DELIVERY MODE
			10/28/2016	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):

pairdocketing@ssiplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte YIN WEI, SUBRAMANIAN IYER,
RICHARD CAMPAGNA, and JAMES WOOD¹

Appeal 2014-008242
Application 12/968,095
Technology Center 2400

Before MICHAEL J. STRAUSS, DANIEL N. FISHMAN, and
JAMES W. DEJMEK, *Administrative Patent Judges*.

FISHMAN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–22.² We have jurisdiction over the pending claims under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

¹ Appellants identify Juniper Networks, Inc. as the real party in interest. App. Br. 3.

² In this Decision, we refer to Appellants' Appeal Brief ("App. Br.," filed February 26, 2014); Appellants' Reply Brief ("Reply Br.," filed July 15, 2014); the Final Office Action ("Final Act.," mailed April 25, 2013); the Examiner's Answer ("Ans.," mailed on May 15, 2014); and the original Specification ("Spec.," filed December 14, 2010).

THE INVENTION

Appellants' invention is directed to "an integrated, multi-service network client for cellular mobile devices." Abstract.

Independent claim 1, reproduced below, is representative:

1. A cellular mobile device comprising:

a transmitter and receiver to send and receive cellular communications in the form of radio frequency signals;

a microprocessor;

an operating system executing on the microprocessor to provide an operating environment of application software;

a multi-service virtual private network (VPN) client registered with the operating system as a single application, wherein the multi-service VPN client comprises:

a security manager integrated within the multi-service VPN client to apply at least one security service to network packets;

a VPN handler having an interface to exchange the network packets with the security manager for application of the security service, wherein the VPN handler is configurable to operate in one of an enterprise mode and a non-enterprise mode, wherein in the enterprise mode the VPN handler establishes a VPN connection with a remote VPN security device and provides encryption services to securely tunnel the network packets between the cellular mobile device and the remote VPN security device, and wherein in the non-enterprise mode the VPN handler directs the network packets to the security manager without application of the encryption services and communicates the network packets to a packet-based network without tunneling the packets; and

a VPN control application that provides a unified user interface that allows a user to configure both the VPN handler and the security manager of the multi-service VPN client.

REFERENCES

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Linderman	US 2003/0131245 A1	July 10, 2003
Weaver et al. (“Weaver”)	US 2004/0148346 A1	July 29, 2004
Gaur et al. (“Gaur”)	US 2005/0198498 A1	Sept. 8, 2005
Makela	US 2005/0229111 A1	Oct. 13, 2005
Sundarrajan et al. (“Sundarrajan”)	US 2006/0195840 A1	Aug. 31, 2006
Cole	US 2008/0081605 A1	Apr. 3, 2008
Yamamoto	US 2010/0017406 A1	Jan. 21, 2010 (PCT filed Sept. 27, 2007)

THE REJECTIONS

Claims 1–4, 10–12, 15, and 18–22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Linderman and Weaver. Final Act. 4–8.

Claims 5–9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Linderman, Weaver, and Sundarrajan. Final Act. 8–10.

Claim 13 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Linderman, Weaver, Sundarrajan, and Makela. Final Act. 10–11.

Claim 14 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Linderman, Weaver, Sundarrajan, Makela, and Yamamoto. Final Act. 11–12.

Claim 16 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Linderman, Weaver, and Gaur. Final Act. 12–13.

Claim 17 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Linderman, Weaver, and Cole. Final Act. 13–14.

ANALYSIS

Only those arguments made by Appellants in the Briefs have been considered in this Decision. Arguments that Appellants did not make in the Briefs are waived. 37 C.F.R. § 41.37(c)(1)(iv).

We are not persuaded by Appellants’ contentions of Examiner error (App. Br. 6–25; Reply Br. 3–9). Except for the Examiner’s findings and reasoning regarding claims 13 and 14 as discussed *infra*, we adopt as our own the findings and reasons set forth by the Examiner in the action from which this appeal is taken (Final Act. 2–14) and as set forth by the Examiner in the Answer (Ans. 2–18). However, we highlight and address specific arguments and findings for emphasis as follows.

Claims 1–4, 6–12, 15, and 18–22

“Single Application”

Appellants contend the Examiner erred in finding the combination of Linderman and Weaver teaches or suggests “a multi-service virtual private network (VPN) client registered with the operating system as a single application,” as recited in claim 1. Appellants argue *registering* a multi-service VPN client as a single application means *installing and executing* the multi-service VPN client as a single application. App. Br. 9. Appellants argue none of the references describe a multi-service VPN client that, as a single application, has the features and capabilities set forth in Appellants’

claims (such as the features of a security manager and a VPN handler, as claimed). *Id.*

Appellants' contention is unpersuasive of Examiner error. We find no specific definition in Appellants' Specification that distinguishes *registering* a multi-service VPN client *as a single application* from integrating Linderman's security features into a security layer (230) as a single module. Ans. 13 (citing Linderman ¶ 109; Figure 2). Given the lack of a relevant limiting definition in Appellants' Specification, the Examiner broadly but reasonably construes the disputed limitation, consistent with the Specification, to encompass Linderman's integration of security features into the security layer (230). *Id.*; *see also In re Amer. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004).

Additionally, the Examiner finds "implementing software in a single application container is a matter of obvious engineering choice." Ans. 13 (citing *In re Larson*, 340 F.2d 965, 969 (CCPA 1965)). We agree. The fact that the claimed multi-service VPN client has both a security manager and VPN handler integrated as a single application is not sufficient by itself to patentably distinguish over the prior art unless there are new or unexpected results. *See Larson*, 340 F.2d 965; *see also In re Dulberg*, 289 F.2d 522, 523 (CCPA 1961). Appellants do not identify a new or unexpected result from such integration.

Therefore, we agree with the Examiner's findings that the combination of Linderman and Weaver teaches or suggests "a multi-service [VPN] client registered with the operating system as a single application," as recited in claim 1.

Appellants next argue the Examiner did not address a security manager that provides at least one security service *separate* from a VPN handler that provides encryption services as claimed, but instead refers to Linderman's VPN security services as *both* the VPN handler and security manager. App. Br. 9–10. Therefore, Appellants argue Linderman's VPN security services alone do not teach the functions set forth in the VPN client as claimed, including the VPN client having “both *a security manager* that provides security services and *a VPN handler* that provides encryption / description services for communicating with a remote VPN security device.” *Id.* (citing Linderman ¶ 109). In support of Appellants' contentions, Appellants direct us to the original disclosure and note that the identified portions of the Specification are “without limitation of the claims.” App. Br. 10–11 (citing Spec. ¶¶ 36 and 46; Figure 4A).

We are unpersuaded the Examiner erred. “Though understanding the claim language may be aided by the explanations contained in the written description, it is important not to import into a claim limitations that are not a part of the claim.” *SuperGuide Corp. v. DirectTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004). Appellants' argument makes clear that the cited portions of the Specification are not intended to limit the claims. We agree and, therefore, decline to import Appellants' examples from the Specification to limit the interpretation of a “single application.”

Furthermore, we find Appellants' argument is not responsive to the Examiner's rejection. The Examiner finds Linderman teaches a security layer (230) that intercepts, directs, and authenticates incoming communications (Ans. 14 (citing Linderman ¶ 77)) and teaches VPN functionality that encrypts and tunnels outbound packets (*id.* (citing

Linderman ¶ 109)). As the Examiner explains, “[w]hether Linderman chooses to name each subroutine in the VPN services or not, does not change the fact that claim 1’s VPN handler and security manager are taught in Linderman's security layer that includes the VPN services.” *Id.* We agree. Thus, Linderman teaches a security layer (230) (the claimed “multi-service VPN client registered with the operating system as a single application”), wherein the security layer (230) comprises functionality that intercepts, directs, and authenticates incoming communications (the claimed “security manager”) and functionality that encrypts and tunnels outbound packets (the claimed “VPN handler”), as claimed.

“Enterprise Mode” vs. “Non-Enterprise Mode”

Appellants argue,

Contrary to the assertion of the final Office Action, any modification of the security layer software of Linderman in view of the teachings of Weaver would not have led one of ordinary skill in the art to Applicant’s claimed invention. That is, any modification of the security layer software of Linderman in view of the teachings of Weaver would not have resulted in a VPN handler configurable to operate in both an enterprise mode in which the VPN handler establishes a VPN connection with a remote VPN security device and provides encryption services to securely tunnel the network packets between the cellular mobile device and the remote VPN security device, and a non-enterprise mode in which the VPN handler directs the network packets to the security manager without application of the encryption services and communicates the network packets to a packet-based network without tunneling the packets. Moreover, any modification to the VPN functions of Linderman that would cause those VPN function to not apply encryption services and to not tunnel packets would, in fact, defeat the entire purpose of

the VPN functions. As such, any such modification would **not** have been obvious.

App. Br. 12. In particular, Appellants argue, although Weaver suggests an instant messaging program that may send unencrypted messages, the combination with Linderman does not make sense. *Id.* at 13. Appellants contend, in the proposed combination, Linderman's client applications would not make use of Weaver's encryption because Linderman already provides application-layer encryption. *Id.*; *see also* Reply Br. 4–5 (citing Linderman ¶¶ 87, 92, 109).

We remain unpersuaded of Examiner error. Initially, we note it is well settled that mere attorney arguments and conclusory statements, which are unsupported by factual evidence, are entitled to little probative value. *In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997); *see also In re De Blauwe*, 736 F.2d 699, 705 (Fed. Cir. 1984). Attorney argument is not evidence. *In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974). Nor can such argument take the place of evidence lacking in the record. *Meitzner v. Mindick*, 549 F.2d 775, 782 (CCPA 1977). Appellants provide only unsupported assertions but fail to identify persuasive evidence that Linderman's client applications would not make use of Linderman's VPN security layer in the proposed combination with Weaver's unencrypted messages.

Furthermore, for similar reasons, we are not persuaded by Appellants' arguments that the proposed combination of Linderman and Weaver would defeat Linderman's entire purpose. The Examiner finds Linderman discloses the recited VPN operations to encrypt tunneled communication data selectively and Weaver discloses enabling or disabling of encryption based on a present mode of communication (enterprise mode or casual mode). Ans. 14–15 (citing Linderman ¶¶ 63, 109 and Weaver ¶¶ 89, 91).

Thus, the Examiner finds the combination teaches or suggests the recited VPN handler. We remind Appellants that the conclusion of obviousness does not demand bodily incorporation of one reference into another, but, instead, the test is what would be suggested to the ordinary skilled artisan by the combined teachings. *In re Keller*, 642 F.2d 413, 425 (CCPA 1981).

Lastly, Appellants argue, to the extent Weaver teaches an IM program that may send encrypted messages, there is no suggestion that would lead one of ordinary skill in the art to modify “Linderman to implement a VPN handler that supports a non-enterprise mode in which packets flow through a VPN handler but that the VPN does not tunnel the packets to a remote VPN security device, as recited in claim 1.” App. Br. 13 (emphasis omitted).

Appellants argue, “the Examiner has not articulated a rational reason as to why one of ordinary skill in the art would have looked to modify the VPN security layer software of Linderman in view of an instant messaging program described by Weaver.” *Id.* at 14; *see also* Reply Br. 6.

In particular, Appellants argue “only by impermissibly using Applicant’s claim 1 as a template to piece together the teachings of Linderman and Weaver does the final Office Action arrive at the combination of Linderman and Weaver allegedly teaching all the elements of independent claim 1.”

Ans. 14.

We remain unpersuaded of Examiner error. The Examiner reasons the ordinary skilled artisan would have been motivated to combine Linderman and Weaver “to allow the user appropriate settings when communicating with different groups.” Final Act. 6 (citing Weaver ¶ 35); *see also* Ans. 16. Thus, the Examiner has articulated a reason for the proposed combination based on rational underpinnings. *See KSR Int’l Co. v.*

Teleflex Inc., 550 U.S. 398, 418 (2007). The Court in *KSR* further held, “the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *Id.* Appellants have not persuasively shown the Examiner’s reasoning to be in error.

For the reasons discussed *supra*, we are unpersuaded of Examiner error. Accordingly, we sustain the Examiner’s rejection of independent claim 1. Independent claims 18, 21, and 22 contain similar limitations and are argued together with claim 1. *See* App. Br. 15–18. Thus, for the same reasons as claim 1, we sustain the rejection of claims 18, 21, and 22. Additionally, we sustain the Examiner’s rejections of dependent claims 2–4, 6–12, 15, 19, and 20, which are not argued separately with particularity. *See id.* at 14, 16, and 19.

Claim 5

Claim 5 depends from claim 1 and further recites wherein the VPN handler comprises a host checker module that “inventories a state of the cellular mobile device and builds a health status report, and wherein the host checker outputs the health status report to the remote VPN security device prior to establishing the VPN connection for determining whether the cellular mobile device is compliant with corporate policies.”

Appellants argue “the health monitoring programs 216 of Sundarrajan suggest user-space programs separate from any VPN client” and, therefore, it would not have been obvious to one of ordinary skill in the art at the time of Appellants’ invention. App. Br. 19.

We are not persuaded by Appellants' arguments. As discussed *supra*, an obviousness analysis need not seek out precise teachings but can take account of the inferences and creative steps employed by a person of ordinary skill in the art. *KSR*, 550 U.S. at 418. The Examiner explains the combination would have been obvious "to find any errors within the device." Final Act. 9. We agree and adopt these findings and Appellants do not persuasively rebut these findings. Thus, we are unpersuaded of Examiner error and we sustain the Examiner's rejection of claim 5.

Claims 13 and 14

Claim 13 depends from claim 1 and further recites, in relevant part, wherein a VPN control application "renders a bookmark window using input controls native to the cellular mobile device." The Examiner relies on Makela in the proposed combination for this additional feature. Final Act. 10–11. The Examiner explains,

Makela teaches rendering and parsing the HTML links using device interface components as a keyboard, a touch screen and voice commands[,] which are part of the handset and not prescribed [sic] by the HTML protocol. The claim does not limit the bookmark window or the input interface into a specific implementation.

Ans. 17 (citing Makela ¶ 96).

Appellants argue, "a keyboard, touch screen and voice commands' is not a VPN control application at all, let alone a VPN control application that . . . renders a bookmark window using input controls native to the cellular mobile device." Reply Br. 8.

We are persuaded by Appellants' argument. The recited input controls are elements rendered on the display such as buttons or check

boxes, by the VPN control application. *See* Spec. ¶¶ 74, 94. The Examiner’s interpretation of “input controls” as reading on hardware elements such as keyboards, the touch-screen, and voice commands is unreasonably broad in view of the Specification.

Thus, we are persuaded the Examiner erred in rejecting claim 13 and, for the same reasons, claim 14 dependent therefrom. Therefore, we do not sustain the rejection of claim 13 and 14.³

Claim 16

Claim 16 depends from claim 1 further reciting wherein the VPN handler “establishes the VPN connection as an Internet Protocol Security (IPSec) connection over User Datagram Protocol (UDP), and wherein the VPN handler includes a compression module that applies Lempel-Ziv (LZ) compression in conjunction with the IPSec connection to tunnel encrypted IP packets to the remote VPN security device.” Appellants argue the mere mention of a related compression algorithm does not disclose or suggest the claimed feature of a VPN handler. App. Br. 23.

We are unpersuaded of Examiner error. At the outset, we note 37 C.F.R. § 41.37(c)(1)(iv) requires more substantive arguments in an appeal brief than a mere recitation of the claim elements and a naked assertion that the corresponding elements were not found in the prior art. *See In re Lovin*, 652 F.3d 1349, 1357 (Fed. Cir. 2011). Additionally, the Examiner finds paragraph 39 of Guar teaches compressing IP datagrams (UDP protocols)

³ Appellants raise other issues regarding claim 14. *See* App. Br. 21–22; *see also* Reply Br. 8–9. We do not reach these other issues but, instead, reverse the rejection of claim 14 solely based on its dependency relationship with claim 13.

using LZ compression, followed by IPsec encryption. Ans. 17–18 (citing Guar ¶¶ 39, 40). Appellants fail to address these findings or otherwise provide sufficient evidence or reasoning that rebut the Examiner’s findings regarding Guar. Therefore, we agree with the Examiner’s findings that Guar teaches or suggests the disputed limitation of claim 16. Accordingly, we sustain the Examiner’s rejection of claim 16.

Claim 17

Claim 17 depends from claim 1 and recites, in relevant part, that “when only a cellular network is available and not a wireless packet-based connection, the VPN handler defers the fast reconnect until application-layer data is received from a user application and ready to be sent via the VPN connection.” The Examiner finds Cole teaches not performing automatic fast reconnect while in a 3G network. Final Act. 13–14 (citing Cole ¶ 67).

Appellants assert paragraph 67 of Cole teaches fast connect, but argue Cole’s teachings are contrary to deferring the fast connect until application-layer data is received from a user application and ready to be sent via a VPN connection when only a cellular network is available and not a wireless packet-based connection. App. Br. 24 (citing Cole ¶ 67).

In response to Appellants’ arguments, the Examiner explains Cole teaches if a device is only connected to a 3G network, then fast reconnects are disabled until suitable settings are present. Ans. 18 (citing Cole ¶ 67). The Examiner further finds paragraph 68 of Cole teaches that the suitable settings include a new application’s connectivity requirements. *Id.* (citing Cole ¶ 68). Appellants do not provide sufficient, persuasive evidence or argument to rebut these additional findings in the Examiner’s Answer.

Appeal 2014-008242
Application 12/968,095

Absent persuasive rebuttal in reply to the Examiner's additional findings, we agree with and adopt the Examiner's unrebutted finding that Cole discloses the disputed limitations as recited in claim 17. Therefore, the Examiner's rejection of claim 17 is sustained.

DECISION

We affirm the Examiner's decision to reject claims 1–12 and 15–22.

We reverse the Examiner's decision to reject claims 13 and 14.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART