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.
14/339,527	07/24/2014	Toni Tammisalo	008351.00002	8204

22907 7590 01/18/2019

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER
LE, THANH T

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
01/18/2019	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):

eofficeaction@bannerwitcoff.com
GPD@bannerwitcoff.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte TONI TAMMISALO and TATU J. YLONEN

Appeal 2018-004781
Application 14/339,527[1]
Technology Center 2400

Before JOHN A. EVANS, CATHERINE SHIANG, and BETH Z. SHAW, *Administrative Patent Judges*.

EVANS, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants seek our review under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1–10, 12–22, and 24–29. App. Br. 17–21 (Claims App'x.). We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.[2]

---

[1] Appellants identify SSH Communications Security OYJ, as the real party in interest. App. Br. 3.

[2] Rather than reiterate the arguments of the Appellants and the Examiner, we refer to the Appeal Brief (filed November 29, 2017, "App. Br."), the Reply Brief (filed April 5, 2018, "Reply Br."), the Examiner's Answer (mailed February 7, 2018, "Ans."), the Final Action (mailed June 8, 2017, "Final Act)," and the Specification (filed July 24, 2014, "Spec.") for their respective details.

STATEMENT OF THE CASE

The claims relate to a method and apparatus for generating a session audit log display. *See* Abstract.

Invention

Claims 1, 17, 20, and 29 are independent. An understanding of the invention can be derived from a reading of illustrative claim 1, which is reproduced below with some formatting added:

> 1. A method comprising:
>
> capturing, by an intermediate data processing device comprising a data capture entity, content of encrypted network connections between client hosts and server hosts in a network system to obtain audit log data in association with at least one session in a computerized system,
>
> generating data for a video presentation based on the captured audit log data, and
>
> causing display of the video presentation of at least a part of the at least one session based on the generated data.

References and Rejections

Lorenzetti	US 2003/0151663 A1	Aug. 14, 2003
Rathus	US 2006/0227992 A1	Oct. 12, 2006
Klassen	US 2007/0124386 A1	May 31, 2007
Meenakshisundaram	US 2007/0168678 A1	July 19, 2007
Li	US 2010/0322251 A1	Dec. 23, 2010
Waugh	US 2012/0102373 A1	Apr. 26, 2012
Olsa	US 2012/0221949 A1	Aug. 30, 2012
Al-Shaykh	US 2012/0324584 A1	Dec. 20, 2012
Cioni	US 2014/0282087 A1	Filed Mar. 12, 2013

1. Claims 1, 2, 4, 5, 7, 9, 12, 14, 15, 20, 22, 24, 26, and 29 stand rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, and Klassen. Final Act. 3–7, 18.

2. Claim 3 stands rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, Klassen, and Cioni. Final Act. 8.

3. Claim 6 stands rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, Klassen, and Li. Final Act. 8–9.

4. Claim 8 stands rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, Klassen, and Al-Shaykh. Final Act. 9–10.

5. Claim 10 stands rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, Klassen, and Rathus. Final Act. 10–11.

6. Claims 13 and 25 stand rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, Klassen, and Meenakshisundaram. Final Act. 11–12, 18.

7. Claims 16, 17, 19, 27, and 28 stand rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, Klassen, and Lorenzetti. Final Act. 12–16, 18.

8. Claims 18 and 21 stands rejected under 35 U.S.C. § 103 as being unpatentable over Olsa, Waugh, Klassen, Cioni, and Lorenzetti. Final Act. 17–18.

ANALYSIS

We have reviewed the rejections of claims 1–10, 12–22, and 24–29 in light of Appellants' arguments that the Examiner erred. We consider

Appellants' arguments *seriatim*, as they are presented in the Appeal Brief, pages 5–16.

CLAIMS 1, 2, 4, 5, 7, 9, 12, 14, 15, 20, 22, 24, 26, AND 29: OBVIOUSNESS OVER OLSA, WAUGH, AND KLASSEN.

Claims 1–10 and 12–16

Appellants argue these claims as a group in view of the limitations of independent claim 1. App. Br. 16.

[C]apturing . . . content of encrypted network connections.

Claim 1 recites, *inter alia*, "capturing, by an intermediate data processing device comprising a data capture entity, content of encrypted network connections between client hosts and server hosts." Appellants contend Olsa fails to teach a data logger that captures encrypted data. App. Br. 9.

The Examiner finds Olsa teaches a capture tool, located between a network and an application, to capture incoming and outgoing data of a client terminal. Final Act. 3. The Examiner finds the terminal is a "Secure Shell" ("SSH") terminal. *Id.* The Examiner takes official notice ("[i]t is known in the art . . .") "that in Secure Shell, traffic between the communicating parties is protected with encryption algorithms." *Id.*

Appellants contend Olsa teaches two embodiments of data capture tools, but that each embodiment only captures plaintext, not encrypted data. App. Br. 8. Appellants argue SSH is not used within a terminal device, rather, the encryption/tunnelling has to be removed before the operating system and any applications and functions running within the terminal can access the data. *Id.* at 9.

The Answer finds:

> "SSH, also known as Secure Socket Shell, is a network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implement the protocol. Secure Shell provides strong authentication and secure encrypted data communications between two computers connecting over an insecure network such as the Internet."

Ans. 3 (quoting http://searchsecurity.techtarget.com/definition/Secure-Shell) (emphasis omitted).[3] The Examiner finds: "[t]herefore, it is clearly known that devices or terminals using SSH exchange encrypted data." Ans. 3.

Appellants quote Olsa: "'SSH is a network protocol . . . that allow[s] data to be exchanged using a secure channel **between** the networked devices.'" Reply Br. 2 (quoting Olsa ¶ 24). But, Appellants argue "SSH is of no use within a terminal, and is not involved in internal processing **within** a terminal of terminal data, as the Office appears to assert." *Id.* According to Appellants, the "capture tool" described in Olsa has no access to the network protocol, and only accesses data **after** it has been received by the terminal and after the SSH encryption has been removed. *Id.*

Olsa discloses neither encryption nor decryption. Olsa discloses:

> The incoming data represents the data input by the user in the terminal during the terminal session and the outgoing data represents the output data of the terminal being provided to the user during the terminal session. The terminal data logger stores the captured data in a data store to allow the terminal session to be recreated via an administrator interface that is separate from the terminal.

Olsa ¶ 13. A person of ordinary skill in the art would not understand that an ordinary user would input encrypted data. Olsa does not disclose encrypted

[3] The techtarget.com website refers to an undated blog.

data, but without so explicitly finding, the Examiner appears to rely upon inherency to supply the missing inherency limitation. Ans. 3. ("Olsa discloses the capture tool captures ***all terminal data***, including incoming and outgoing data").

Although inherency can supply a missing claim limitation in an obviousness analysis, the limitation at issue *necessarily* must be present to be inherently disclosed in a reference. *See PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1194–96 (Fed. Cir. 2014). Here, even where encrypted data may be transmitted over the internet, it is not been shown that inherently the server and the terminal operate on encrypted data. *See* Olsa ¶ 13 ("The incoming data represents the data input by the user").

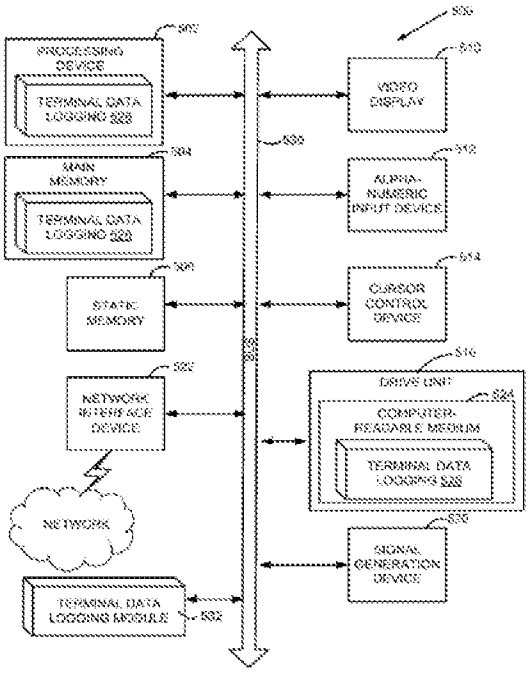

FIG. 5

Olsa's Figure 5 illustrates a diagrammatic representation of a machine in the exemplary form of a computing system for terminal data logging.

Olsa discloses in Figure 5 a diagrammatic representation of a machine in the exemplary form of a computing system for terminal data logging the machine may operate as a server or client. Olsa ¶ 42. Figure 5 illustrates many of the devices that may optionally comprise the machine. *Id.* Olsa discloses the machine may be networked to other machines in a LAN, an intranet, an extranet, or the Internet. *Id.* Figure 5 shows a network connected to "network interface device 522." Appellants contend

> [t]here is no evidence or suggestion in Olsa that SSH would be used within a terminal device, or that the terminal data logger of Olsa would capture and process **encrypted** data before SSH tunnelling has been removed from incoming data, or after the SSH protocol has been applied to outgoing data.

App. Br. 9. We agree. Device 512 is described as a keyboard (Olga ¶ 45) with no suggestion that data is encrypted prior to its application to the bus. Similarly, there is no disclosure that any device attached to the bus applies or accepts encrypted data.

We find no evidence Olsa teaches "capturing . . . content of encrypted network connections," as recited in independent claim 1. Independent claims 17, 20, and 29 contain commensurate limitations. Therefore, we decline to sustain the rejections of claims 1–10, 12–22, and 24–29.

DECISION[4]

The rejection of claims 1–10, 12–22, and 24–29 under 35 U.S.C. § 103 is reversed.

REVERSED

[4] Because we do not sustain the Examiner's rejection of claims 1–10, 12–22, and 24–29 for the reasons discussed *supra*, we need not address Appellants' additional arguments. *See Beloit Corp. v. Valmet Oy*, 742 F.2d 1421, 1423 (Fed. Cir. 1984) (Finding an administrative agency is at liberty to reach a decision based on "a single dispositive issue.").