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.
12/882,431	09/15/2010	Lawrence B. Tropp	365334US91	2929

22850 7590 01/30/2019

OBLON, MCCLELLAND, MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
JENKINS, BENJAMIN A

ART UNIT	PAPER NUMBER
2445	

NOTIFICATION DATE	DELIVERY MODE
01/30/2019	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):

patentdocket@oblon.com
OBLONPAT@OBLON.COM
iahmadi@oblon.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte LAWRENCE B. TROPP and
THOMAS R. VOLPERT

Appeal 2018-004023
Application 12/882,431[1]
Technology Center 2400

Before MICHAEL J. STRAUSS, IRVIN E. BRANCH, and
PHILLIP A. BENNETT, *Administrative Patent Judges*.

BENNETT, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 47–62 and 64–66. Claims 1–46 and 63 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

[1] Appellants' Brief ("App. Br.") identifies UPONUS Technologies, LLC as the real party in interest. App. Br. 1.

CLAIMED SUBJECT MATTER

The claims are directed to an apparatus and associated methodology for managing content control keys. Spec., Title. In the claimed embodiments, identical random number tables are provided to both a sending and receiving device. These random number tables are used to allow for the two devices to "exchange secret session keys in symmetric encryption without transmitting the actual secret session key from the sending device to the receiving device." Spec. ¶ 21. The secret session key is selected from within the random number table by the sending device. Rather than sending the key, the device sends information describing the location in the table that was used to create the session key. *Id.* The receiving device can use that information to generate the same session key. *Id.* Claim 47, reproduced below, is illustrative of the claimed subject matter:

> 47. A method for secure communication between a sending device and a receiving device, comprising:
>
> providing a same random number table to both the sending device and the receiving device;
>
> providing a same symmetric encryption algorithm to both the sending device and the receiving device;
>
> for each piece of data of a plurality of pieces of data to be transmitted:
>
> selecting, at the sending device and directly from the random number table, a secret key as a subset of the random number table, the secret key being identified by location information identifying a location of the subset within the random number table;
>
> encrypting, at the sending device, the piece of data using the secret key and the symmetric encryption algorithm to generate encrypted data;
>
> transmitting, from the sending device to the receiving device, the encrypted data, a user key code and the location information;

determining, at the receiving device, whether the user key code received from the sending device matches a user key code stored on the receiving device;

when the user key code received from the sending device matches the user key code stored on the receiving device:

identifying, at the receiving device, the secret key in the random number table based on the location information, and

decrypting, at the receiving device, the encrypted data using the secret key and the symmetric encryption algorithm; and

when the user key code received from the sending device does not match the user key code stored on the receiving device, terminating communication between the sending device and the receiving device without identifying the secret key at the receiving device.

App. Br. 12–13 (Claims Appendix).

REFERENCES

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

Hoskinson	US 5,455,862	Oct. 3, 1995
Atalla	US 5,960,086	Sept. 28, 1999
Tan	US 6,490,353 B1	Dec. 3, 2002
Bowman	US 6,751,736 B1	June 15, 2004

P. Baronti et al., "Wireless Sensor Networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," pp. 1655–1695, Computer Communications 30 (2007)

G. Kessler, "An Overview of Cryptographic Methods," CRC Pressm LLC (2000).

REJECTIONS

Claims 47, 48, 50, 51, 53, 54, 56–62, 64, and 66 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Atalla and Hoskinson. Final Act. 15–23.

Claim 49 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Atalla, Hoskinson and Tan. Final Act. 23.

Claim 52 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Atalla, Hoskinson, and Bowman. Final Act. 24.

Claim 55 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Attila, Hoskinson, and Baronti. Final Act. 24–25.

Claim 65 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Atalla, Hoskinson, and Kessler. Final Act. 25–26.

ISSUE

Has the Examiner erred in determining that Attila teaches, suggests, or otherwise renders obvious selecting a secret key "for each piece of data of a plurality of pieces of data to be transmitted," as recited in claim 47?

ANALYSIS

Appellants' claim 47 recites a series of encryption and transmission operations which are performed "for each piece of data of a plurality of pieces of data to be transmitted." App. Br. 12 (Claims Appendix). The issue before us is whether the Examiner properly relies on Attila for this limitation.

In rejecting independent claim 47, the Examiner finds that Attila teaches performing the recited encryption and transmission operations "for each piece of data of a plurality of pieces of data to be transmitted." Final Act. 16 (citing Attila col. 2, l. 67 – col. 3, l. 1; col. 2, ll. 10–11, 59–60). The Examiner finds that "Attila discloses using a key only once, and then discarding it." Final Act. 3 (citation omitted). The Examiner explains that Appellants' use of a new key for "each piece of data to be transmitted" is "analogous to a one-time pad, which is analogous to Attila's teaching of one-time use." Final Act. 3. The Examiner further finds that Attila discloses using a different key for each communication session, and that generating a new key for each session renders this limitation obvious. In the Answer, the Examiner further explains that Attila's disclosure of the use of a new key for each transaction also teaches the "for each piece of data" limitation. Ans. 4 (Attila col. 12, 19–20).

Appellants argue that Attila is deficient because "though Attila generally describes changing session keys frequently, Attila falls short of describing that the session keys should be changed each time a piece of information is transmitted. At best, Attila describes that changing the session key for every *session* is sufficient." App. Br. 8. Appellants argue that changing the key for each session is not the same as "for each piece of data of a plurality of pieces of data to be transmitted" because "the level of ordinary skill in the art was such that a communication session, and particularly a secure communication session, was commonly regarded to require transmission of more than just one piece of data or just one packet." App. Br. 9. Appellants assert this argument is supported by the Declaration of John M. Shea, submitted as evidence under 37 C.F.R. § 1.132, which

states that "one of ordinary skill in the art of computer science would . . . consider a 'session' to typically include communication of multiple pieces of data." App. Br. (Exhibit A at 2).

We are not persuaded by Appellants' argument.[2] We do not find the Shea Declaration persuasive because even if fully credited, it does not assert that a communication session *necessarily* includes multiple pieces of data. Rather, the Shea Declaration states only that a session *typically* includes communication of multiple pieces of data. This assertion does not exclude the possibility that a session can include a single piece of data. Thus, the Shea Declaration implicitly acknowledges the possibility that Attila's teaching of generating a new key for each session is encompassed by the disputed limitation.

Moreover, we agree with the Examiner that Attila's disclosure of generating a new key for each transaction teaches or suggests the disputed limitation. Specifically, Attila describes "[t]he use of a simple and fast process to encrypt and decrypt the information to be transmitted as part of each transaction made practical by the use of a new encryption key for each new transaction." Attila col. 12, ll. 18–21. At least one dictionary defines "transaction" as including "[a]n input message to a system that, because of the nature of the real-world event or activity it reflects, requires to be regarded as a single unit of work and must either be processed completely or

[2] Although not critical to our ultimate decision, we observe the specification does not define the phrase "piece of data." In fact, this phrase appears nowhere in the Specification. Appellants provide no proposed definition of the phrase. Thus, it is somewhat unclear whether the phrase should be interpreted such that each "piece of data" is a bit of data, a byte of data, a packet of data, a file, or something else.

rejected." *Transmission*, A Dictionary of Computing (6th ed.) 2008. Thus, a transaction is a "single unit of work" such as, for example, a single piece of data. As such, Attila's description of providing a new key for each transaction teaches or suggests doing so "for each piece of data of a plurality of pieces of data to be transmitted," as recited in claim 47. Accordingly, we are not persuaded the Examiner erred in rejecting claim 47 under 35 U.S.C. § 103(a), and we sustain the rejection. Because Appellants present no separate arguments for patentability of any other claim, we treat claim 47 as representative, and the remaining claims fall along with claim 47.

DECISION

We affirm the Examiner's rejections of claims 47–62 and 64–66.

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

AFFIRMED