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.
15/923,403	03/16/2018	Cedric Staub	S156-0323US	3604

126350   7590   09/03/2020

Lee & Hayes, P.C./Square
601 West Riverside Avenue
Suite 1400
Spokane, WA 99201

EXAMINER
NIGH, JAMES D

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
09/03/2020	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):

lhpto@leehayes.com

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE
————————

BEFORE THE PATENT TRIAL AND APPEAL BOARD
————————

Ex parte CEDRIC STAUB and ANTHONY BISHOPRIC
————————

Appeal 2020-004278
Application 15/923,403
Technology Center 3600
————————

Before JUSTIN BUSCH, BETH Z. SHAW, and JOYCE CRAIG,
Administrative Patent Judges.

SHAW, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the
Examiner's decision to reject claims 1–8, 10–15, and 17–22. *See* Final Act.
1. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

CLAIMED SUBJECT MATTER

The claims are directed to detecting alterations of journal data structures. Claim 1, reproduced below, is illustrative of the claimed subject matter:

1. A method for preventing tampering with two or more account journals associated with a merchant, the method performed by one or more computer servers associated with a network-based accounting service, the method comprising:

providing, by the one or more computer servers associated with the network-based accounting service and to a client device operable by the merchant, an interface enabling the merchant to record transactions in the two or more account journals of the merchant, wherein the two or more account journals are managed by the network-based accounting service;

receiving, via a first input to the interface and by the one or more computer servers associated with the network-based accounting service, a first request to record a first transaction of a temporally ordered sequence of transactions associated with the merchant, wherein the first request specifies first transaction data to be recorded in two or more journal entries and a transaction signature created with a private key of an asymmetric cryptographic key pair of the merchant;

verifying, via the one or more computer servers associated with the network-based accounting service, the transaction signature using a public key of the asymmetric cryptographic key pair to confirm that the first request is from the merchant;

adding, via the one or more computer servers associated with the network-based accounting service, a first journal entry in a first account journal of the two or more account journals to record at least a portion of the first transaction data;

adding, via the one or more computer servers associated with the network-based accounting service, a second journal entry in a second account journal of the two or more account journals to record at least another portion of the first transaction data, wherein the second journal entry at least partially offsets the first journal entry;

determining, via the one or more computer servers associated with the network-based accounting service, a first authentication tag of the first journal entry based at least in part on a first sequential key, wherein the first authentication tag comprises a message authentication code determined based on a plurality of fields of the first journal entry and the first sequential key;

associating, via the one or more computer servers associated with the network-based accounting service, the first authentication tag with the first journal entry;

calculating, via the one or more computer servers associated with the network-based accounting service, a second sequential key by applying a one-way function to the first sequential key;

discarding, via the one or more computer servers associated with the network-based accounting service, the first sequential key;

receiving, via a second input to the interface and by the one or more computer servers associated with the network-based accounting service, a second request to record a second transaction, wherein:

the second request specifies second transaction data to be recorded in two or more additional journal entries;

the two or more additional journal entries offset one another in different account journals of the two or more account journals; and

the second transaction is immediately subsequent to the first transaction in the temporally ordered sequence of transactions;

adding, via the one or more computer servers associated with the network-based accounting service, a third journal entry in the first account journal to record at least a portion of the second transaction data;

determining, via the one or more computer servers associated with the network-based accounting service, a second authentication tag of the third journal entry based at least in part on the second sequential key;

associating, via the one or more computer servers associated with the network-based accounting service, the second authentication tag with the third journal entry;

discarding, via the one or more computer servers associated with the network-based accounting service, the second sequential key; and

verifying, via the one or more computer servers associated with the network-based accounting service, an integrity of the first account journal based on at least one of the first authentication tag or the second authentication tag.

REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
Bellare	Mihir Bellare & Bennet Yee, *Forward-Security in Private-Key Cryptography*, Topics in Cryptogoly – CT-RSA '03	2003
Kelsey	J. Kelsey et al., *Signed Syslog Messages*, Internet Engineering Task Force Proposed Standard RFC 5848, https://tools.ietf.org/html/rfc5848	2010
Marson	Giorgia Azzurra Marson & Bertram Poettering, *Even more practical secure logging: Tree-Based Seekable Sequential Key Generators*	2015
Pillay	Iresh Pillay, *What is triple entry accounting?* https://www.linkedin.com/pulse/what-triple-entry-accounting-iresh-pillay (last viewed August 19, 2019)	2017

REJECTIONS

Claims 1–5 are rejected under 35 U.S.C. § 103 as being unpatentable over Kelsey, Marson, Bellare, and Pillay. Final Act. 3.

Claims 6–8, 10, 11, 13–15, and 17–22 are rejected under 35 U.S.C. § 103 as being unpatentable over Marson and Pillay. Final Act. 10.

Claim 12 is rejected under 35 U.S.C. § 103 as being unpatentable over Kelsey, Marson, and Pillay. Final Act. 20.

OPINION

We conclude the Examiner did not err in finding one skilled in the art would have recognized the combination of references teaches or suggests the disputed limitations in claims 1–8, 10–15, and 17–22. We refer to, rely on, and adopt the Examiner's findings and conclusions set forth in the Final Rejection and Answer. *See* Final Act. 2–21; Ans. 2–9.

Appellant argues Marson does not teach or suggest "determining, via the one or more computer servers associated with the network-based accounting service, a first authentication tag of the first journal entry based at least in part on a first sequential key, **wherein the first authentication tag comprises a message authentication code determined based on a plurality of fields of the first journal entry and the first sequential key**," as claim 1 recites. Appeal Br. 14. In particular, Appellant argues Marson does not teach or suggest generating an "authentication tag" based on a sequential key and a "plurality of fields of the first journal entry and the first authentication key." *Id.* at 14–15 (emphasis omitted).

The Examiner finds that

Marson teaches that the authentication tag is a forward-secure variant of a message authentication code, or MAC on page 2 in the section titled "Forward-secure cryptography for log file protection" and at section 3.3 where a key for a particular epoch is generated using what is described by Marson as the Evolve algorithm. The syslog messages themselves are described by Kelsey in RFC 5848 as consisting of structured data elements (section 1 at the bottom of page 4 continuing onto page 5 and further described in sections 3 and 9.1). Marson references the Kelsey document in the reference section at item 11 regarding the May 2010 draft of RFC 5848. Clearly Marson and those skilled in the art understood that the MAC generated using Marson's sequential key was a signed syslog message and therefore constituted a plurality of fields based on the data

5

structure that is part of a syslog as defined by RFC 5848. Appellant's argument does not go into any particular detail as to what Appellant views as deficient in Marson and Examiner only can presume that the emboldened "plurality of fields" language is what is being contested by Appellant as the argument does not go beyond the restatement of the claim. Therefore Examiner does not see where Appellant has shown any clear error on the part of the Examiner.

Ans. 5–6.

In reply, Appellant argues that there is no discussion in Marson about using the structured data elements of a syslog message to generate a message authentication code. Reply Br. 4. However,

[w]hen a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. . . . [I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 417 (2007). Marson need not have a precise teaching to use the structured data elements of a syslog to generate a message authentication code to render the claim obvious, for such an addition would have been within ordinarily skilled artisans' knowledge when accounting for the inferences and creative steps that these artisans would have employed. *See id.* at 416. In "the context of secure logging," Marson describes protecting locally stored log files using a message authentication code that equips all occurring log messages with an authentication tag. Marson, section 3.3. As the Examiner explains in the Answer, and we agree, syslog messages are described by Kelsey as consisting of structured data elements, and Marson references Kelsey regarding protecting log files. Marson, 3; Ans. 5.

Appellant additionally argues that Pillay does not teach "providing, by the one or more computer servers associated with the network-based accounting service and to a client device operable by the merchant, an interface enabling the merchant to record transactions in the two or more account journals of the merchant, wherein the two or more account journals are managed by the network-based accounting service." Appeal Br. 15; Reply Br. 5–6. Appellant argues that "due to the fundamentals of blockchain technology," i.e., because blockchains are decentralized, Pillay cannot teach the "providing," as claimed. Appeal Br. 15–16. Appellant argues that claim 1 recites that the account journals are managed by a central authority because the preamble recites the servers are associated with the network-based accounting service. *Id.* Yet, as the Examiner points out, and we agree, the claim does not require a "central authority." *See* Ans. 6, 7. Rather, the claim refers to "one or more computer servers." Although Appellant argues on page 6 of the Reply Brief that the bookkeeping and accounting operations described are performed in a way that is not done by distributed peer devices, we are not persuaded by this argument because it is not commensurate in scope with claim 1, which does not preclude the use of distributed servers. Accordingly, this argument is not commensurate in scope with the claim language.

Finally, Appellant argues that it would not have been obvious to combine Kelsey, Marson, and Pillay to teach the subject matter of claim 1. Appeal Br. 16; Reply Br. 6–7. As the Examiner determines, however, Marson refers directly to Kelsey, and Appellant does not directly address the motivation statements made in the Final Rejection in the Appeal Brief. Ans. 7. Appellant also argues that "the Office appears to be relying upon . . . a problem . . . rather than recognition of a solution to such a problem" and

"the currently cited documents would have led one of ordinary skill in the art in a direction different than the solution recited in claim 1." Appeal Br. 16–17. We are not persuaded by this argument because:

> [T]he problem motivating the patentee may be only one of many addressed by the patent's subject matter. The question is not whether the combination was obvious to the patentee but whether the combination was obvious to a person with ordinary skill in the art. Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

KSR, 550 U.S. at 420. Other than a general assertion without evidentiary support in the Reply Brief, (*see* Reply Br. 7), Appellant has not demonstrated that the Examiner's proffered combination would have been "uniquely challenging or difficult for one of ordinary skill in the art," and, therefore, we agree with the Examiner that the proposed modification would have been within the purview of the ordinarily skilled artisan. *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 418).

Accordingly, we sustain the rejection of claim 1. For the same reasons, we sustain the rejection of claims 2–5, for which Appellant presents the same or essentially the same arguments as claim 1. *See* Appeal Br. 17.

Claim 6

Regarding independent claim 6, Appellant reiterates some of the same arguments as made for claim 1, and we are not persuaded by those arguments for the same reasons as discussed above with respect to claim 1. *See* Appeal Br. 18–19. Additionally, Appellant argues that Marson's "system events" are not "transactions" that are associated with a "network-based accounting service," as recited in claim 6. Appeal Br. 17–18.

Appellant argues Marson does not teach or suggest "adding, by the server computing system, a first journal data entry to a first journal data structure to record at least a portion of the first transaction data," because Marson more generally describes computer logs and does not describe a "data structure" that is "associated with an account journal," as claim 6 requires. *Id.* Appellant provides insufficient evidence proving that the Specification or claims limit "transactions" or "data structures" in a way that, under a broad but reasonable interpretation, is not encompassed by Marson's teachings of log files recording a variety of system events. *See* Final Act. 10–11 (citing Marson, sections 1, 3.3.); Ans. 8. Accordingly, we sustain the rejection of claim 6.

For the same reasons, we sustain the rejections of the remaining pending claims, for which Appellant presents the same or essentially the same arguments. *See* Appeal Br. 19–20. Despite nominally arguing these claims separately, Appellant reiterates similar arguments made in connection with claims 1 or 6, and alleges that the additional cited prior art fails to cure those purported deficiencies. *Id.* We are not persuaded by these arguments for the reasons previously discussed.

CONCLUSION

The Examiner's rejections are affirmed.

DECISION SUMMARY

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–5	103	Marson, Pillay, Kelsey, Bellare	1–5	
6–8, 10, 11, 13–15, 17–22	103	Marson, Pillay	6–8, 10, 11, 13–15, 17–22	
12	103	Marson, Pillay, Kelsey	12	
Overall Outcome			1–8, 10–15, 17–22	

TIME PERIOD FOR RESPONSE

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