

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

BLACKBERRY CORP.,
Petitioner,

v.

FACEBOOK, INC.,
Patent Owner.

Case IPR2019-01596
Patent 7,228,432 B2

Before MIRIAM L. QUINN, SCOTT C. MOORE, and JASON M. REPKO,
Administrative Patent Judges.

QUINN, *Administrative Patent Judge.*

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

I. INTRODUCTION

Blackberry Corp. (“Petitioner”) filed a Petition (Paper 1, “Pet.”), requesting *inter partes* review of claims 1 and 3–6 of U.S. Patent No. 7,228,432 B2 (Ex. 1001, “the ’432 patent”). Facebook, Inc. (“Patent Owner”) timely filed a Preliminary Response (Paper 6, “Prelim. Resp.”).

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the petition “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.” For the reasons stated below, we determine that Petitioner did not demonstrate a reasonable likelihood of prevailing with respect to at least one challenged claim. We, therefore, do not institute *inter partes* review.

A. Related Matters

The ’432 patent is the subject of a district court proceeding in the Northern District of California, captioned *Facebook, Inc. v. BlackBerry Limited.*, Case No. 4:18-cv-05434-JSW (N.D. Cal.). Pet. 2.

B. The ’432 Patent

The ’432 patent relates to “providing security for a computer system, which includes generating a request for a file.” Ex. 1001, Abstract. The ’432 patent explains that security systems in a network of computers may be used to prevent unauthorized intrusion or attacks from outside sources. *Id.* at 1:18–22. The ’432 patent further explains that the computers in the network are nevertheless vulnerable because unknown viruses may still attack and the security functions impact the performance of the Central Processing Unit (CPU) of the computer. *Id.* at 1:25–33. The ’432 patent,

therefore, describes a dedicated security processor that receives the request for a file and accesses the requested file. *Id.* at 1:40–44. “Then, the dedicated security processor validates the requested file and provides the file to another processor, if the requested file is validated.” *Id.* Figure 2, reproduced below, illustrates a computer system.

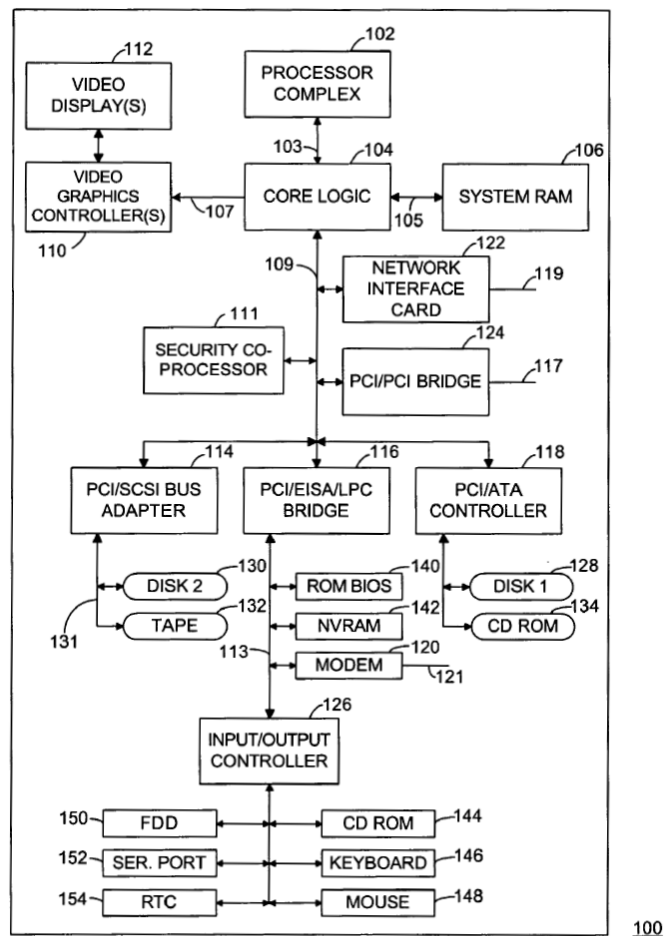


Fig. 2

Figure 2 depicts a block diagram of a computer system 100 comprising processor complex 102 and security co-processor 111. The security co-processor is dedicated to providing security functions to

computer system 100. *Id.* at 15–16. Security co-processor 111 validates functions and activities before they are executed. *Id.* at 4:11–15. Because the security co-processor 111 performs the security functions and activities, it frees the use of the CPU cycles on the processor complex 102 for other computing activities. *Id.* at 4:17–20.

C. Illustrative Claims

Petitioner challenges claims 1 and 3–6 of the '432 patent. Claim 1 is independent and reproduced below:

1. A method of providing security for a computer system, the method comprising the acts of:
 - generating a request for a file;
 - receiving the request at a dedicated security processor;
 - using the dedicated security processor to access the file;
 - using the dedicated security processor to validate the requested file.
 - providing the file to an other processor, if the requested file is validated;
 - validating a user access to execute the request; and
 - enabling the other processor to continue processing the file, if the user access is validated.

Ex. 1001, 10:7–18.

D. Asserted Prior Art

Petitioner relies on the following references as prior art (Pet. 4):

- 1) *Peinado*: U.S. Patent No. 7,225,333 B2, filed as Exhibit 1004; and
- 2) *McKelvey*: U.S. Patent No. 5,896,499, filed as Exhibit 1005.

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 3–4):

Claims Challenged	35 U.S.C. §	Basis
1 and 3–6	§ 102(e)	Peinado
1 and 3–6	§ 103	Peinado and McKelvey

Petitioner further relies on the Declaration of Jeffrey S. Chase, Ph.D. to support its patentability challenge. Ex. 1003 (“Chase Declaration”).

Patent Owner proffers a Declaration of James A. Storer to challenge Petitioner’s asserted grounds of unpatentability. Ex. 2001 (“Storer Declaration”).

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 invention of the ’432 patent “would have had a Bachelors of Science degree in computer or electrical engineering, or equivalent, and 2–3 years of relevant experience working with computer security technology.” Pet. 8–9. Patent Owner states that “[a] person of ordinary skill in the art . . . would have had approximately the level of education and experience identif[ied] by Petitioner, or a similar level of education and/or experience, with somewhat more education substituting for somewhat less work experience and vice versa.” Prelim. Resp. 4 (citing Storer Decl. ¶ 16). Given the lack of dispute, and for purposes of this decision, we adopt Petitioner’s definition of the level of ordinary skill in the art, as it is consistent with the level of skill in

the art reflected in the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

B. Claim Construction

In an *inter partes* review proceeding, a claim of a patent is construed using the same standard used in federal district court, including construing the claim in accordance with the ordinary and customary meaning of the 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). Petitioner proposes that the term “dedicated security processor” means “a processor dedicated to providing security functions.” Pet. 9–10. Patent Owner states that in the co-pending litigation, the parties have agreed to this construction, and, therefore, Patent Owner does not dispute the proposed construction. Prelim. Resp. 4–5.

For purposes of this decision, we adopt the construction of “dedicated security processor” proposed by Petitioner, as stated above, and agreed to by Patent Owner in the co-pending litigation. The remainder of the claim we interpret in accord with the claim’s ordinary meaning to one skilled in the art at the time of invention, in light of the teachings of the specification and the prosecution history, and do not find it necessary to provide any express claim constructions. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’”) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

C. Anticipation Ground: Peinado

Petitioner contends that claims 1 and 3–6 are anticipated by Peinado. Pet. 12–25. With regard to claim 1, Patent Owner argues that Peinado does not disclose the “dedicated security processor” and the “other processor” because Peinado describes a single processor. Prelim. Resp. 11–17. We are persuaded by Patent Owner’s argument. Before we turn to our analysis, we provide an overview of Peinado.

1. Overview of Peinado

Peinado is directed to a “security processor” operable in normal and preferred modes, and includes a security kernel when the processor enters into preferred mode. Ex. 1004, Abstract. The context of Peinado is a Digital Rights Management (DRM) system. *Id.* at 1:26–29. In such a system, when a user attempts to render the digital content on a computer, the rendering application invokes the DRM system on the user’s computer. *Id.* at 2:65–3:1. The DRM either directs the user to a license server to obtain a license to render the digital content, or transparently obtains the license without any further action by the user. *Id.* at 3:1–6. The DRM system on the user’s computer includes a black box, which when rendering the digital content, decrypts the decryption key and license terms. *Id.* at 3:54–56. Figure 13 of Peinado is reproduced below.

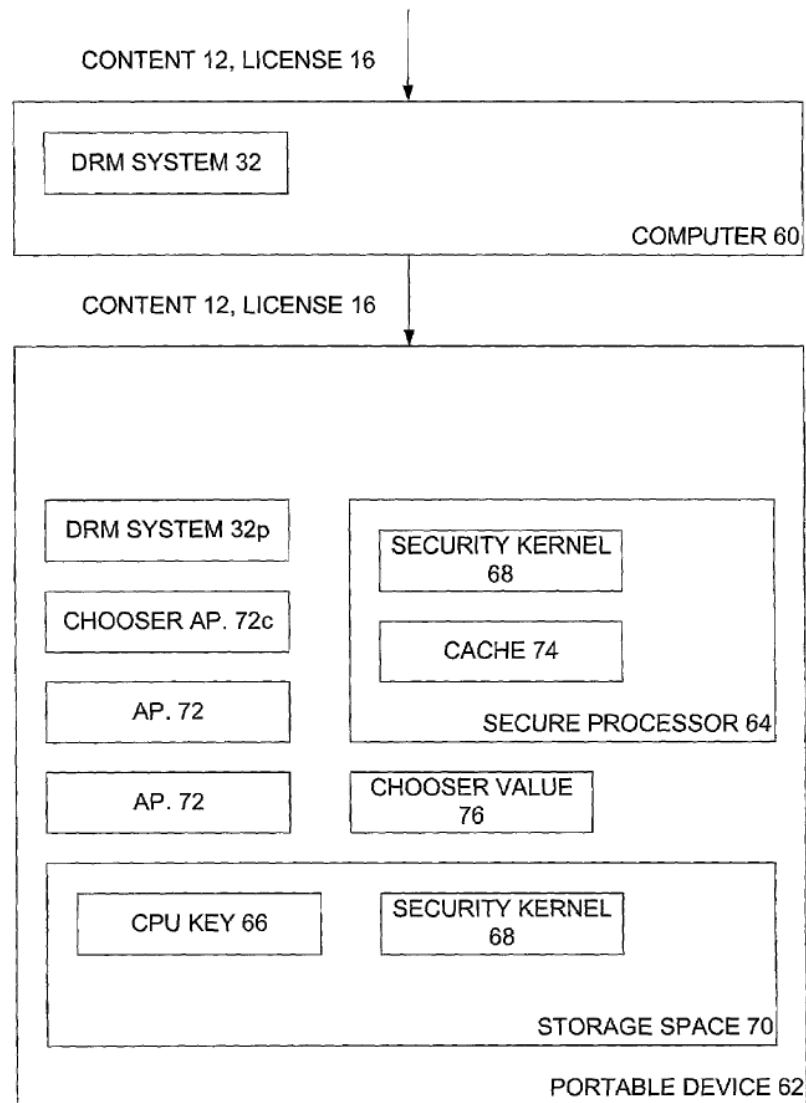


Fig. 13

Figure 13 shows a block diagram of a portable device, coupled to a computer for downloading digital content and a digital license from a computer 60. *Id.* at 3:24–26. In particular, computer 60 downloads digital content 12 and license 16. *Id.* at 35:44–49. Thereafter, content 12 and license 16 are downloaded from computer 60 to portable computing device 62. *Id.* at 35:50–52. Portable device 62 includes DRM system 32p with the

functionality necessary to authenticate portable device 62, to facilitate the download, and to render content 12 on portable device 62 in accordance with license 16. *Id.* at 36:53–60. Portable device 62 and security processor 64 “must be of a type that substantially completely prevents a content thief from performing nefarious acts that would allow obtaining of content 12 therein in an unencrypted form or decryption keys.” *Id.* at 37:2–6. Thus, secure processor 64 is constructed to run only authorized code. *Id.* at 37:10–11. Secure processor 64 is operable in a normal mode and a preferred mode, where security kernel 68 can access CPU key 66 only during the preferred mode. *Id.* at 37:56–58. Security kernel 68 instantiates the application on portable device 62 and authenticates the application using CPU key 88. *Id.* at 38–60. Once the security kernel finishes instantiating/authenticating the application, processor 64 enters normal mode and the CPU key becomes inaccessible. *Id.* at 38:5–7.

2. Analysis

Petitioner contends that Peinado anticipates independent claim 1. In particular, with respect to the “dedicated security processor” limitation, Petitioner contends that Peinado discloses a DRM system that runs on secure processor 64 (sometimes referred to also as security processor 64). Pet. 15 (citing Ex. 1004, 3:62–67, 37:11–17, 45:8–25). According to Petitioner, Peinado discloses that the DRM system can be implemented in connection with “multi-processor systems” and “network PCs.” *Id.* at 16 (citing Ex. 1004, 6:29–30; Chase Decl. ¶ 48). Petitioner further argues that, because Peinado states that the “invention may be practiced in distributed

computing environments,” Peinado then discloses that the DRM system is a “trusted component” in a “multi-processor system” or a “distributed computing environment.” *Id.*

We do not agree with Petitioner’s contention. As Patent Owner correctly notes, Peinado’s DRM system and the rendering application are both implemented on a computing device with a single processor. Prelim. Resp. 13. As stated above in the summary of Peinado, security processor 64 runs DRM system 32p in the portable device to authenticate the digital content downloaded from another computer. Ex. 1004, 37:62–66. The same DRM system 32p renders the digital content on the portable device. *Id.* at 36:53–62. The claim requires that the “dedicated security processor” validate the file and user access. The claim also requires that the “dedicated security processor” provide the file to “an other processor” that continues processing the file after the user has been validated. There is no “providing” step in Peinado’s security processor 64 embodiment. The same processor performs both the validating and the processing of the file after validation.

Petitioner also points to the disclosure of the decrypted content being provided to the rendering application. *See* Pet. 19. But that “providing” is (1) not shown occur in the embodiment of security processor 64 and (2) not shown to involve “an other processor.” Pointing to another *application* receiving the content in a completely different *embodiment* in Peinado is not sufficient to show that Peinado discloses the limitation. Accordingly, we find that the Petition does not show adequately that Peinado *anticipates* claim 1 of the ’432 patent.

Petitioner’s additional argument—that some embodiments of Peinado disclose a “multi-processor system” or a “distributed computing environment” such that the DRM system would be implemented as such—is not persuasive. Such an argument relies on a disclosure of Peinado concerning the various permutations that could happen in a computer environment with conventional personal computers. Ex. 1004, 6:15–51. Peinado, however, fails to explain how the DRM system implemented in security processor 64 performs the validation of the file and the user request, and provides the file to some other processor running the rendering application. In sum, Peinado does not explain an architecture in which one processor executes the DRM system and another processor processes the validated content. *See* Prelim. Resp. 16–17. Indeed, “it is not enough that the prior art reference discloses part of the claimed invention, which an ordinary artisan might supplement to make the whole, or that it includes multiple, distinct teachings that the artisan might somehow combine to achieve the claimed invention.” *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). “Differences between the prior art reference and a claimed invention, however slight, invoke the question of obviousness, not anticipation.” *Id.*

Petitioner also argues that, to the extent the term “dedicated security processor” is broader than the proposed construction, Peinado’s description of the DRM system as a “trusted component or mechanism” would satisfy the limitation. Pet. 16–17. Petitioner’s argument is not persuasive. Petitioner’s position that mere mention of the DRM functionality satisfies the requirement of a dedicated security processor eviscerates the claim

requirement, according to the agreed claim construction, of two distinct processors. At best, Peinado states that it may store software modules in remote processing devices. *See* Pet. 20 (citing Ex. 1004, 6:31–34). It says nothing about executing those modules in different processors.

Nevertheless, and contrary to the statements in the Petition, we are persuaded that Peinado fails to disclose an embodiment in which “a rendering application is running on a processor distinct from the DRM system or dedicated processor.” *See* Pet. 20 (citing Chase Decl. ¶ 54).

Consequently, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in its contention that claim 1, and challenged dependent claims 3–6, are anticipated by Peinado.

D. Obviousness Ground Based on Peinado and McKelvey

The Petition states that “to the extent that the Board finds that Peinado’s disclosure is not sufficiently clear, it would, at a minimum, have been obvious to combine Peinado with McKelvey to arrive at a subject matter within the scope of ’432 claims 1 and 3–6.” Pet. 26 (citing Chase Decl. ¶ 65). In particular, Petitioner relies on McKelvey’s disclosure of an embedded security processor dedicated to network communications security tasks. *Id.* (citing Ex. 1005, Abstract). Petitioner argues that because Peinado discloses that the DRM system should be a trusted component or mechanism, such a disclosure would “immediately suggest to a POSITA that the DRM system should be implemented in the form of a dedicated security processor, like that disclosed in McKelvey.” *Id.* at 26–27 (citing Chase Decl. ¶ 68). By way of a rationale, Petitioner argues that there were known

benefits of using dedicated processors for security functions and that such a dedicated processor “would have allowed for a more secure firewall against malicious or insecure content by physically isolating the primary processor from said content until it had been validated.” *Id.* at 27 (citing Chase Decl. ¶¶ 69, 24–30). Finally, Petitioner argues that using a dedicated security processor would also have reduced CPU load by shifting security tasks to a separate processor. *Id.*

Before we address Petitioner’s obviousness contentions, we provide a summary of McKelvey.

1. Overview of McKelvey

The title of McKelvey, “Embedded Security Processor,” alludes to McKelvey’s description of using an embedded security processor in addition to a main processor in a computer network. Ex. 1005, Abstract. McKelvey’s solution to providing a more secure network is in the context of using “firewalls.” *Id.* at 2:56–58. McKelvey defines a “firewall” as a “separate computer system with a dedicated microprocessor that can be used to provide certain types of security. The firewall computer is usually placed into the computer network so that it is logically located between the protected system and the unsecure network.” *Id.* at 2:58–63. Despite the firewall’s usefulness, its use also adds complexity and other security risks. *Id.* at 3:26–57. Thus, McKelvey implements an expansion board that has an embedded security processor used in conjunction with the main processor. *Id.* at 4:7–13. The embedded security processor performs security functions as follows:

The embedded security processor is controlled by the main processor and intercepts all communications from external untrusted or unverified network systems (i.e., unsecure networks) and verifies that the attempted communication traffic is permissible before allowing the external network traffic to access the main processor via the system bus, or other networked computer resources accessible via a secure network.

Id. at 4:13–20. Figure 1 of McKelvey is reproduced below.

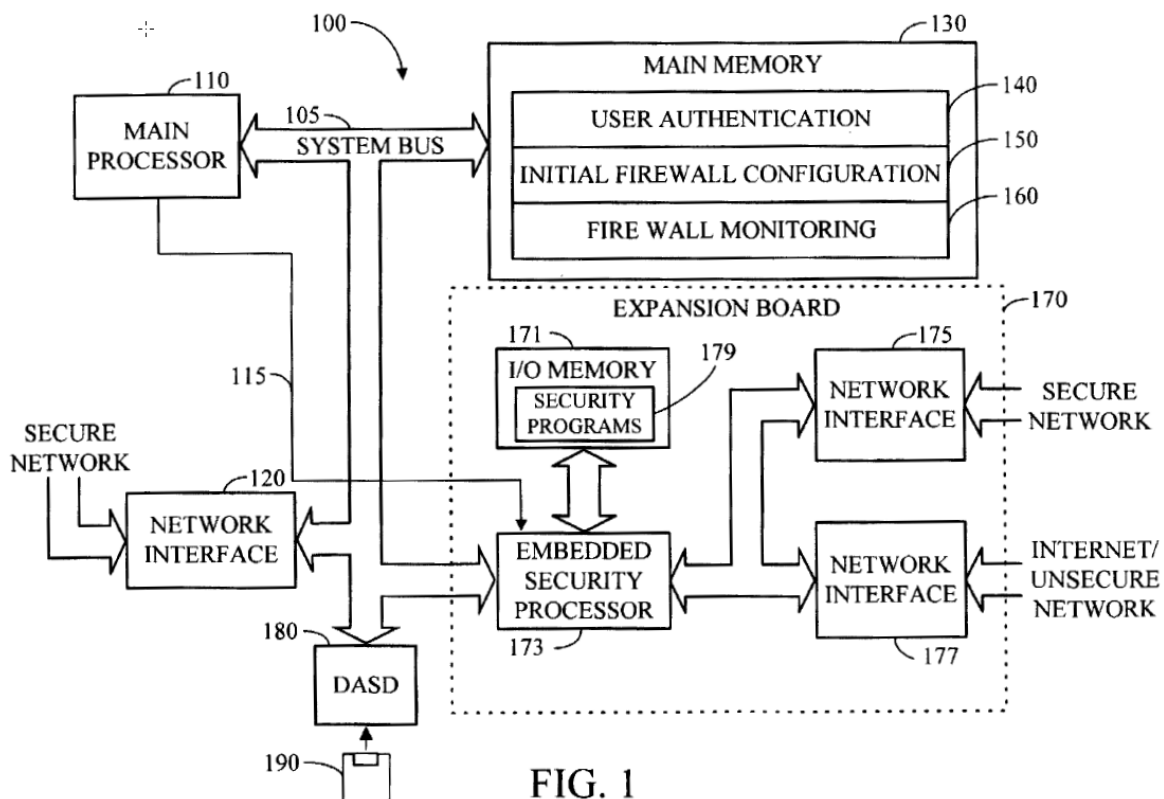


FIG. 1

Figure 1 is a block diagram of computer system 100 showing embedded security processor 173 in expansion board 170. *Id.* at 5:48–55. Main processor 110 is implemented in a single Central Processing Unit (CPU). *Id.* at 6:45–50. Embedded security processor 173 is also

implemented as a single CPU. *Id.* at 7:29–30. Main processor 110 uses control signal 115 to start, stop, and otherwise control embedded security processor 173 as determined by the security needs of system 100. *Id.* at 8:17–21. In order to provide firewall security protection against unwanted traffic over an unsecure network, such as the Internet, network interface 177, located on expansion board 170, is connected to the unsecure network. *Id.* at 8:12–15. All communication traffic between main processor 110 and the unsecure network must pass through embedded security processor 173, which blocks all unwanted traffic, while allowing desired traffic to pass through. *Id.* at 25–29.

2. Analysis

Patent Owner challenges Petitioner’s contention that it would have been obvious to combine the teachings of Peinado and McKelvey. Prelim. Resp. 25–34. First, we address Patent Owner’s challenge of Petitioner’s assertion that Peinado’s “trusted” environment for the DRM system would “immediately suggest” implementing some or all of the DRM system as the embedded security processor of McKelvey. Prelim. Resp. 29–30. As Patent Owner correctly notes, Peinado’s “trusted” environment refers to Peinado’s use of a black box that performs the decryption and encryption for the DRM system. *Id.* at 30 (citing Ex. 1004, 3:18–22). Peinado describes that the “trusted” DRM system is one that can be self-authenticating. Ex. 1004, 3:18–22. This black box resides in DRM system 32 (in the user’s computing device as shown in Figure 4 of Peinado). Petitioner does not explain that, nor do we find any suggestion of, a self-authenticating feature

itself becoming a reason for a person of ordinary skill in the art to implement separate processors. The word “trusted” (involving self-authentication as explained above) in Peinado suggests, at best, that an authentication or certificate procedure is in place, such as that described in column 23 of Peinado. Ex. 1004, 23:10–24:55. In particular, each black box has a version number and a certificate with a digital signature, which are the mechanisms by which the license server determines if it should “trust” the black box. *Id.* at 23:44–54. The Petition does not explain any other feature of the “trust” in Peinado that would reasonably suggest, much less “immediately suggest,” that a separate processor would be implemented for reasons of “trust.”

Second, we address Patent Owner’s challenge of Petitioner’s assertion that the combination would have allowed a more secure firewall by “physically isolating the primary processor” from malicious or unsecure content. *See* Pet. 27. Patent Owner argues that McKelvey’s proposed solution of an embedded processor for firewall functions solves a different problem and provides a solution different from those recognized in Peinado. Prelim. Resp. 25–27. For instance, Patent Owner points out that Peinado has no need for a firewall processor that isolates the content from the rendering application because, in Peinado, the content is downloaded to the user computer *before* the DRM system is invoked. *Id.* We agree that the functionality of the DRM system’s validation and license check is at odds with the purported use of McKelvey’s embedded security processor. In order for McKelvey’s security processor to work as McKelvey intended, and as Petitioner alleges (for isolating unsecure content), Peinado would have to be modified to invoke the DRM system, using a separate processor, *before*

the rendering application downloads and accesses the content. Otherwise, the content is not physically isolated from the rest of the user computer. Petitioner does not advocate any such modification and, more importantly, we find no reason to implement such a change in Peinado. Therefore, we do not find persuasive Petitioner's argument that McKelvey's physical-isolation benefit would be a reason to combine the teaching of the embedded security processor with Peinado's teachings of the DRM system.

Third, we address Petitioner's contention of CPU-load reduction as a reason to combine. Patent Owner argues that Petitioner's assertion has no factual support. Prelim. Resp. 32–33. There is, for instance, no evidence that adding a separate processor would solve a CPU-load problem in Peinado. *Id.* Nor is there evidence that McKelvey solves a CPU-load problem by implementing the embedded (and separate) security processor. *Id.* According to Patent Owner, the change of Peinado to include a separate processor is a substantial change, increasing costs and complexity of the system, without any indication that there is a tangible benefit that outweighs the detrimental impact to the design of Peinado. *Id.* at 33–34. Specifically, on this last point, Patent Owner argues that Peinado's simplicity and cost of running the rendering application and the DRM system in the same processor would have to be weighed against the cost and complexity of adding a separate processor to run the DRM system, as well as considering the impact to the form factor and the necessary programming. *Id.* at 27.

We agree with Patent Owner that on the present record, Petitioner's bare assertion of reducing CPU load is insufficient to show a reasonable motivation to combine. There are drawbacks and benefits attributable to the

proposed combination of teachings. Petitioner has asserted a generic benefit of CPU-load reduction by shifting security tasks to another processor. *See* Chase Decl. ¶ 69. Petitioner, however, does not explain this assertion vis-à-vis the drawbacks of making such a change to Peinado’s architecture. We are persuaded by Patent Owner’s argument that a person of ordinary skill in the art must consider the disadvantages as well as the advantages. Prelim. Resp. 27. Neither the Petition nor the Chase Declaration provide an analysis of these considerations, which is the relevant inquiry as to whether a person having ordinary skill in the art would be motivated to combine references despite drawbacks that the combination might present. *Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000). We are also persuaded that the Petition does not provide sufficient information for us to perform the relevant analysis. As the *Winner* court recognized, the Board must weigh the benefits and drawbacks of the modification against each other, to determine whether there would be a motivation to combine. *Id.* at 1349 n.8; *see also Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1331–32 (Fed. Cir. 2019) (concluding that the Board’s proper analysis considered the design tradeoffs to determine whether on balance they yield an “unappetizing combination.”). At this juncture, Patent Owner presents persuasive argument that the combination of teachings would indeed result in drawbacks that are not explained compared against a conclusory and hindsight-looking benefit of CPU-load reduction.

Given the present record, we are not persuaded that Petitioner’s proffered rationale is sufficient to satisfy the institution burden. Consequently, and for the reasons stated above, we determine that Petitioner

IPR2019-01596
Patent 7,228,432 B2

has not demonstrated a reasonable likelihood of prevailing on its assertion that claim 1, and dependent claims 3–6, would have been obvious over Peinado and McKelvey.

III.ORDER

Accordingly, it is hereby:

ORDERED that the Petition is *denied*.

IPR2019-01596
Patent 7,228,432 B2

PETITIONER:

Robert C. Mattson
Alexander B. Englehart
Oblon, McClelland, Maier & Neustadt, LLP
CPDocketMattson@oblon.com
CPDocketEnglehart@oblon.com

PATENT OWNER:

Heidi L. Keefe
Andrew C. Mace
COOLEY LLP
hkeefe@cooley.com
amace@cooley.com