

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO INC.,
Petitioner,

v.

CUPP COMPUTING AS,
Patent Owner.

IPR2021-01237
Patent 10,951,632 B2

Before THOMAS L. GIANNETTI, GARTH D. BAER, and
SHARON FENICK, *Administrative Patent Judges*.

BAER, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. BACKGROUND

Trend Micro Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1, 7, 9, 16, 22, and 24 (the “challenged claims”) of U.S. Patent No. 10,951,632 B2 (Ex. 1101, the “’632 patent”). Paper 1 (“Pet.”). CUPP Computing AS (“Patent Owner”) filed a Preliminary Response. Paper 9. Pursuant to 35 U.S.C. § 314, we instituted this *inter partes* review as to all of the challenged claims and all grounds raised in the Petition. Paper 16 (“Institution Dec.”).

Following institution, Patent Owner filed a Response. Paper 25 (“PO Resp.”). Subsequently, Petitioner filed a Reply to Patent Owner’s Response (Paper 28, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 30, “PO Sur-reply”).

On October 18, 2022, we held a consolidated oral hearing with IPR2021-01236, also involving the ’632 patent. A transcript of the hearing is included in the record. Paper 36 (“Hearing Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision issued pursuant to 35 U.S.C. § 318(a). For the reasons we discuss below, we determine that Petitioner has proven by a preponderance of the evidence that all challenged claims of the ’632 patent are unpatentable.

B. RELATED PROCEEDINGS

The parties identify the following district court proceeding concerning the ’632 patent: *CUPP Cybersecurity LLC v. Trend Micro, Inc., et al.*, No. 3:20-cv-03206 (N.D. Tex.). Pet. 1–2; Paper 7. In addition, Petitioner challenges claims 1, 9, 16, and 24 of the ’632 patent in IPR2021-01236 (the

“1236 IPR”). A Final Written Decision in the 1236 IPR is being entered concurrently with this Decision.

A closely related patent, U.S. Patent No. 9,843,595 (the “’595 patent”)¹ was before the Board in IPR2019-00765 (the “765 IPR”). A Final Written Decision in the 765 IPR, finding all challenged claims of the ’595 patent unpatentable, was entered on August 25, 2020. Ex. 1003. That Decision was appealed to the Federal Circuit and affirmed on November 16, 2022. *CUPP Computing AS v. Trend Micro Inc.*, 53 F.4th 1376 (Fed. Cir. 2022).

C. REAL PARTY-IN-INTEREST

The Petition identifies Trend Micro as the real party-in-interest. Pet. 1. Patent Owner identifies CUPP Computing AS as the real party-in-interest. Paper 7, 1.

D. THE ’632 PATENT

The ’632 patent describes a system and method for providing data and device security between external and host devices. Ex. 1101, 1:30–33. According to the patent, mobile devices are more vulnerable to attacks by malicious code when traveling outside an enterprise network. *Id.* at 1:61–65. The patent thus describes “a small piece of hardware [a ‘mobile security system’] that connects to a mobile device and filters out attacks and malicious code.” *Id.* at 5:45–47. The patent explains that “[u]sing the mobile security system, a mobile device can be protected by greater security

¹ The ’632 patent is a continuation (through a chain of continuations) of the ’595 patent (Ex. 1104), and shares a common specification with the ’595 patent. Ex. 1101, 1:8–26.

and possibly by the same level of security offered by its associated corporation/enterprise.” *Id.* at 5:49–52.

This system is illustrated in Figure 3 of the '632 patent, which follows:

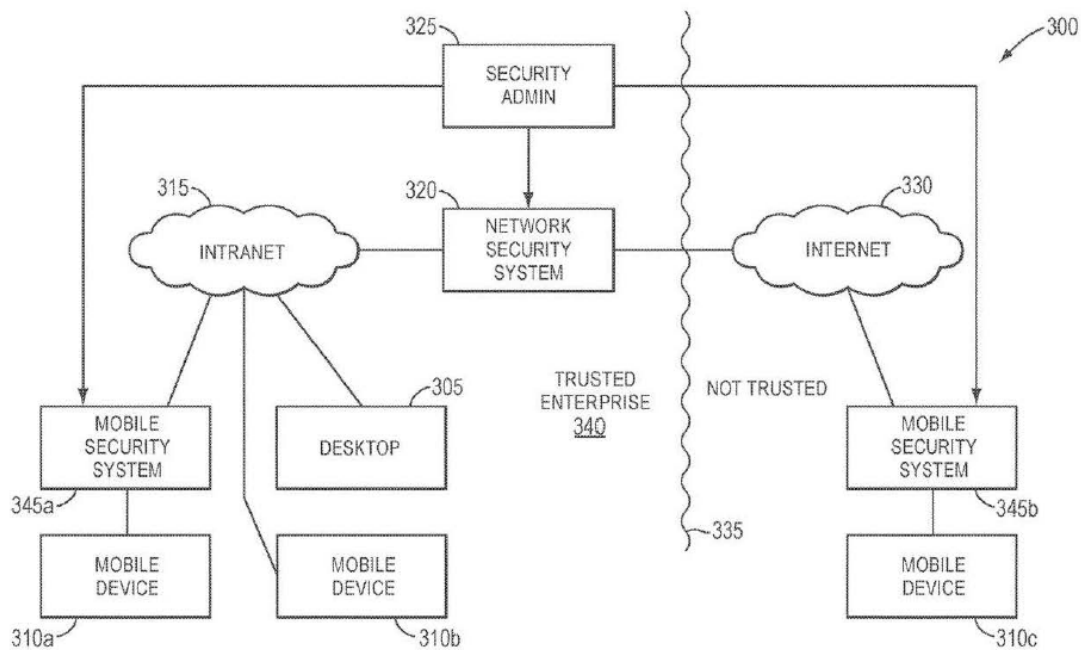


FIG. 3

Figure 3 of the '632 patent is a block diagram of a network system.

Ex. 1101, 5:53–54. Network system 300 includes desktop 305, first mobile device 310a, and second mobile device 310b. *Id.* at 5:54–56. First mobile device 310a is within trusted enterprise network 340 and is coupled to the enterprise’s intranet 315 via mobile security system 345a. *Id.* at 5:56–59.

Figure 3 further shows mobile device 310c that has travelled outside trusted enterprise network 340 and is coupled to untrusted internet 330 via mobile security system 345b. *Id.* at 6:3–5. This mobile device may be in use by an employee of trusted enterprise network 340 who is currently on travel. *Id.* at

6:6–7. Security administrator 325 manages mobile security systems 345a and 345b and network security system 320 to assure that they include the most current security protection. *Id.* at 6:7–11.

The '632 patent also describes a wake module configured to wake a mobile device from a power management mode. Ex. 1101, 21:63–64, Fig. 18. According to the patent, a power management mode “is a mode wherein the mobile device conserves power, usually after a predetermined period of inactivity (e.g., no input from a mouse and keyboard).” *Id.* at 21:64–67. During power management mode, the mobile device may reduce or eliminate power to one or more mobile device components such as a display and/or hard drive. *Id.* at 21:67–22:3.

E. ILLUSTRATIVE CLAIM

Claims 1 and 16 are independent. Claim 1 is representative of the challenged claims. Claim 1 recites²:

- [1.0] A security system, comprising:
 - [1.1] security system memory;
 - [1.2.a] a communication interface configured to communicate with a mobile device and configured to communicate over a network with a security administrator device,
 - [1.2.b] the mobile device including a mobile device processor and including a security agent configured to cooperate with the security system,
 - [1.2.c] the security administrator device having a security administrator processor different than the mobile device processor, the mobile device being remote from the security administrator device,

² Paragraph numbering provided by Petitioner has been added.

[1.2.d] the mobile device being a first computer system, the security system being a second computer system, the security administrator device being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems; and

[1.3] a security system processor being different than the mobile device processor and different than the security administrator processor, the security system processor being configured to:

[1.4.a] store in the security system memory at least a portion of wake code, the wake code being configured to detect a wake event and to send a wake signal to the mobile device in response to detecting the wake event,

[1.4.b] the security agent of the mobile device being configured to receive the wake signal, the security agent of the mobile device being configured to wake at least a portion of the mobile device from a power management mode in response to receiving the wake signal, the security agent of the mobile device being configured to perform security services after the at least a portion of the mobile device has been woken;

[1.5] detect a particular wake event;

[1.6] prepare a particular wake signal in response to detecting the particular wake event; and

[1.7.a] send the particular wake signal to the mobile device in response to detecting the particular wake event,

[1.7.b] the security agent of the mobile device being configured to wake the at least a portion of the mobile device in response to receiving the particular wake signal and being configured to perform particular security services after the at least a portion of the mobile device has been woken.

Ex. 1101, 31:15–58.

F. ASSERTED GROUNDS OF UNPATENTABILITY

Petitioner asserts the challenged claims are unpatentable on the following grounds:

Claims Challenged	Basis (35 U.S.C.) ³	Reference(s)
1, 7, 9, 16, 22, 24	§ 103(a)	Gordon, ⁴ Gardner ⁵
7, 22	§ 103(a)	Gordon, Gardner, Chang ⁶
9, 24	§ 103(a)	Gordon, Gardner, Meenan ⁷

Pet. 4. In addition, Petitioner submits the Declaration of Dr. Markus Jakobsson (Ex. 1121, “Jakobsson Decl.”). Patent Owner submits the Declaration of Michael T. Goodrich, Ph.D. (Ex. 2011, “Goodrich Decl.”).

II. PRELIMINARY MATTERS

A. LEVEL OF ORDINARY SKILL

Petitioner contends “[a] person of ordinary skill in the art at the time of the alleged invention of the ’632 patent (i.e., August 4, 2008) . . . would have had a bachelor’s degree in computer science, electrical engineering, or

³ Because the parties agree that the challenged claims of the ’632 patent have an effective filing date before March 16, 2013, we apply the pre-AIA (“America Invents Act”) version of § 103. Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

⁴ U.S. 7,818,803 B2, Oct. 19, 2010 (Ex. 1107, “Gordon”).

⁵ U.S. 2006/0272020 A1, Pub. Nov. 30, 2006 (Ex. 1108, “Gardner”).

⁶ U.S. 2011/0264931 A1, Pub. Oct. 27, 2011 (Ex. 1109, “Chang”).

⁷ U.S. 2006/0101277 A1, Pub. May 11, 2006 (Ex. 1111, “Meenan”).

a comparable field of study, plus at least two years of professional experience with computer security systems, or the equivalent.” Pet. 13.

Patent Owner contends “[a] person of ordinary skill in the art of the ’632 Patent would be someone with a bachelor’s degree in computer science or a related field and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or a related field.” PO Resp. 7. These formulations are similar, differing mainly in the specific reference, in Patent Owner’s formulation, to “an advanced degree in computer science or a related field” as a possible alternative to experience in the field.

We adopt Patent Owner’s description as it is consistent with the prior art and patent specification before us and supported by credible expert testimony. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). However, our decision would be the same under either formulation.

B. CLAIM CONSTRUCTION

In an *inter partes* review, the claims of a patent shall be construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims 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); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005). Under that standard, and absent any special definitions, we give claim terms their ordinary and customary meaning, as would be understood by one of ordinary skill in the art at the time of the invention. *See In re Translogic Tech., Inc.*, 504 F.3d

1249, 1257 (Fed. Cir. 2007). Any special definitions for claim terms must be set forth with reasonable clarity, deliberateness, and precision. *See In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

We construe claim terms only as relevant to the parties' contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

1. power management mode (all challenged claims)

This term has been construed in the 765 IPR and in district court litigation involving the '595 patent as "a mode where the mobile device conserves power." Pet. 13–14; PO Resp. 17. There is no dispute over this construction. *See* Ex. 1106, 2.⁸ The construction is supported by the '632 patent specification. *See* Ex. 1101, 21:62–64 ("A power management mode is a mode wherein the mobile device conserves power."). We, therefore, agree with this construction and we adopt it for this decision.

2. security administrator device (all challenged claims)

Petitioner contends "the plain and ordinary meaning of this term includes a device that performs security administration." Pet. 14 (citing Jakobsson Decl. ¶ 65). Petitioner asserts that "[t]his is consistent with the '632 patent's disclosure that the security administrator device 325 may perform various security administration tasks." *Id.*

⁸ Unless otherwise indicated, citations to exhibits use the page numbers assigned by the parties, not the original page numbers.

Patent Owner responds that “[t]his term is defined in the ’632 Patent as a device that manages the security of a security system.” PO Resp. 14 (citing Ex. 1101, 6:7–11) (emphasis omitted). Patent Owner asserts that “Petitioner’s proposed construction includes the phrase ‘security administration,’ but it is unclear as Petitioner leaves unsaid what ‘security administration’ does and does not encompass.” *Id.* at 16.

We are persuaded to adopt Petitioner’s construction. Petitioner’s construction reflects its position that “[i]n no place do the claims recite that the ‘security administrator device’ must manage the ‘security system.’” Pet. Reply 12. We agree that a security administrator device need not “*manage*” the security of a security system, as Patent Owner asserts. PO Resp. 14. Our construction is consistent with the term’s plain language as well as the ’632 patent claims and is supported by expert testimony. Jakobsson Decl. ¶ 65.

As Petitioner points out, the claims themselves make no mention of managing the security of a security system. Pet. Reply 12. Claim 1 recites that the security system is “configured to communicate over a network with a security administrator device.” Ex. 1101, 31:18–19. Claim 16 recites that the security administrator device is “a third computer system,” but does not recite a relationship between the security administrator device and the security system. *Id.* at 32:61–63; *see also* Jakobsson Decl. ¶ 65 (“The plain and ordinary meaning of this term includes a device that performs security administration.”).

Petitioner’s construction also is consistent with the ’632 patent’s disclosure that the security administrator device may perform various security administration tasks. Pet. 14; Ex. 1101, 24:55–57 (describing

security administrator 325 as an “administrator device”). As Petitioner points out, “[a]lthough management is a type of administration, administration includes other activities more broadly related to running a system, such as maintaining routing tables.” Pet. Reply 12 (citing Ex. 1101, 12:28–30; Ex. 1125, 3).

We do not agree with Patent Owner’s argument that Petitioner’s proposed construction is “unclear.” PO Resp. 16. As Petitioner points out, the relationship between the security system and the security administrator device is recited in the claims. Pet. Reply 12. The claims do not recite that the security administrator device manages the security device, “let alone manage[s] the security of the security system.” *Id.*

We do not agree with Patent Owner’s argument that the term “security administrator device” is “defined in the ’632 Patent.” PO Resp. 14 (citing Ex. 1101, 6:7–11). We are not convinced that the reference to this phrase in the ’632 patent specification cited by Patent Owner sets forth with sufficient “clarity, deliberateness, and precision” a lexicographic definition. *See Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998); *In re Paulsen*, 30 F.3d at 1480. Instead, Patent Owner’s argument is an attempt to incorporate limitations from a particular embodiment that are not recited in the claims. *See* Pet. Reply 13–14.

We, therefore, do not adopt Patent Owner’s proposed construction for this term. Adopting Petitioner’s construction, we construe the term as “a device that performs security administration.” Pet. 14; Jakobsson Decl. ¶ 65.

3. particular wake event/particular wake signal/particular security services (all claims)

Patent Owner contends that “[t]aken as a whole, these claim elements recite a technique whereby a wake event triggers a particular *type* of wake signal which triggers the mobile device’s security for a particular *type* of security service.” PO Resp. 7–8. Citing Merriam-Webster’s dictionary, Patent Owner contends that “[t]his interpretation is consistent with the plain and ordinary meaning of the word ‘particular,’ which is ‘of, relating to, or being a single person or thing.’” *Id.* at 8 (citing Ex. 2012, 3).

Petitioner responds that “a ‘particular’ wake signal includes one that is distinguishable from other wake signals, such as a wake signal that occurs at a specific time.” Pet. Reply 1. Therefore, “[a] wake signal that occurs at a specific time is a specific, single, and individual wake signal, distinguishable from wake signals that occurred at other times. Thus, it is a ‘particular’ wake signal.” *Id.* at 2. Petitioner argues that the Board should reject Patent Owner’s argument “that these claim terms should be limited to a ‘particular type of’ wake signal, wake event, and security service.” *Id.* at 4–5.

We agree with Petitioner that the claims should not be limited to a particular *type* of wake event or signal. The claims themselves recite a “particular wake signal,” not a particular *type* of wake signal. The same is true for wake events. Patent Owner’s argument would, therefore, require us to rewrite the claims to make a distinction between what Patent Owner refers to as “generic” wake signals and events and “particular” wake signals and events. *See* Hearing Tr. 38:26–39:7, 41:6–19. This distinction is not reflected in the claims or specification.

At the oral hearing, Patent Owner’s counsel was questioned by the panel exploring the differences between particular and generic wake events. Hearing Tr. 50:10–51:3. Ultimately, Patent Owner’s counsel acknowledged that a wake event occurring at every hour could be a particular wake event:

[THE BOARD:] What if there was a wake event that was wake at noon and a wake event that was wake at midnight? . . . [W]ould one of those qualify as a particular wake event?

[PATENT OWNER’S COUNSEL:] Yeah. I believe each one because that’s the -- what’s described and what’s claimed is that you -- there is a particular wake event which has to be detected. It’s not limited to only one, so it could be -- it could be every hour. *There could be a particular wake event which is each hour.* So, you know, *that’s the particular wake event.* Or it could be just, like you said, at noon -- or at noon or at midnight. *Those would each be a particular wake event.*

And then what the claim says or requires is that for each particular wake event, there has to be a particular wake signal that’s associated with that particular. And it could be that what you do at noon or what you do at midnight *are the same*, or it could be different. And then from whatever that particular wake signal is for that particular wake event, then you have a particular security service that’s offered.

Hearing Tr. 50:10–51:3 (emphasis added).

Patent Owner argues that “[u]nder Petitioner’s interpretation, the Challenged Claims would have the same meaning with and without the word ‘particular’ because *every* detected wake event would occur at some point in time.” PO Resp. 11; *see also* PO Sur-reply 1–2 (“Petitioner’s proposal . . . should be rejected because it renders the word ‘particular’ superfluous.”). We disagree that under Petitioner’s construction, the term “particular” would be meaningless or superfluous. We agree with Petitioner

and find that “[a] signal sent at time T_1 is not the same signal sent at time T_2 .” Pet. Reply 2. As Petitioner explains, “[a]lthough the signals may have the same form, each is individually identifiable.” *Id.* Two wake signals of the same form sent at the same time would not be “particular” wake signals because they would not be distinguishable on the basis of time. *Id.* at 2–3. Thus, Petitioner’s interpretation provides a meaningful identification of particular wake events and wake signals. For the reasons given, we adopt Petitioner’s construction of these claim elements.

This construction will be further discussed in Section III.A.1.i *infra*, in connection with our consideration of the prior art.

4. security agent (all claims)

Patent Owner contends that “[t]he plain and ordinary meaning of the term ‘security agent’ is a security system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda and so as to effect what it senses in the future.” PO Resp. 12 (emphasis omitted). For support, Patent Owner relies on a paper by Franklin titled “Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents.” *Id.* (citing Ex. 2013, 4).

Petitioner responds that “Patent Owner’s construction comes from Franklin’s definition of ‘autonomous agent,’ not ‘security agent’ or ‘agent.’” Pet. Reply 6. Petitioner explains that “Franklin . . . acknowledges that some agents may not be autonomous.” *Id.* (citing Ex. 2013, 6). Petitioner presents several “broader” dictionary definitions of “agent.” *Id.* at 7 (citing Exhibits 1124 (from “Barron’s Dictionary of Computer and Internet Terms”), 1125 (from “Concise Oxford English Dictionary”) and 1126 (from “Merriam-Webster’s Collegiate Dictionary”). Petitioner contends that

Merriam-Webster’s definition (“a computer application designed to automate certain tasks”)⁹ has been adopted as an “accepted ordinary meaning” in another proceeding. *Id.* at 8.

Petitioner contends that Patent Owner’s construction is unsupported by the intrinsic evidence. Pet. Reply 9–10. Petitioner explains that in the ’632 patent, the cited security agent does not act “in pursuit of its own agenda” because it sometimes acts on behalf of the mobile security system. *Id.* at 9 (citing Ex. 1101, 28:25–28; 28:44–53).

We agree with Petitioner that Patent Owner’s construction based on Franklin is not supported by the intrinsic evidence. First, neither the written description nor the claims of the ’632 patent themselves recite “autonomous agent.” Nor do Patent Owner’s references to the specification demonstrate that the agent described in the ’632 patent acts “in pursuit of its own agenda.” PO Resp. 12–13. In addition, Franklin presents “autonomous” as a property of a special type of agent, one where the agent “exercises control over its own actions.” Ex. 2013, 5–6. For the reasons given, we are not persuaded that the “security agent” recited in the ’632 patent claims and described in the specification is an “autonomous” agent as discussed in Franklin. We, therefore, do not adopt Patent Owner’s construction for “security agent.” Instead, we adopt the plain and ordinary meaning best expressed by Merriam-Webster, namely, “a computer program designed to automate certain tasks.” Ex. 1126, 3.

⁹ The correct quote from the dictionary is “a computer *program* designed to automate certain tasks.” Ex. 1025, 3 (emphasis added). We do not regard this minor error as affecting our analysis.

The laptop and wireless security module also communicate with monitoring center 70 via a wireless connection. *Id.* at Fig. 2, 5:7–12, 15:12–15.

III. ANALYSIS OF THE CHALLENGED CLAIMS

A. OBVIOUSNESS OF CLAIMS 1, 7, 9, 16, 22, AND 24 BASED ON GORDON AND GARDNER

1. Claim 1

Petitioner asserts that the combination of Gordon and Gardner teaches each element of claim 1. Pet. 18–44. Petitioner supports its analysis with testimony by its expert, Dr. Jakobsson. Jakobsson Decl. ¶¶ 67–128.

a. Preamble [1.0]

The preamble of claim 1 recites a “security system.” Petitioner identifies Gordon’s host monitoring system and monitoring center 70 as the claimed “security system.” Pet. 19–22. Patent Owner’s Response does not challenge this contention. We find that for the reasons given, Petitioner demonstrates that Gordon teaches the preamble of claim 1.¹⁰

b. Claim element 1.1

Claim element 1.1 calls for a “security system memory.” Petitioner contends Gordon teaches this feature because Gordon’s monitoring system includes a monitoring server 3 that is a physical computer, which “inherently and necessarily has a memory.” *Id.* at 22–23. Patent Owner’s Response does not challenge this contention. We find that for the reasons given, Petitioner demonstrates that Gordon teaches element 1.1.

¹⁰ We do not express an opinion on whether the preambles of the ’632 patent claims are limiting.

c. Claim element 1.2.a

This claim element calls for “a communication interface configured to communicate with a mobile device and configured to communicate over a network with a security administrator device.” Petitioner identifies Gordon’s laptop computer A3 as the claimed “mobile device.” *Id.* at 24. Petitioner explains further that Gordon refers to Gardner, and that Gardner discloses additional detail about host monitoring system C, including a “‘web-based or network based console’ . . . that remotely accesses the host monitoring system C.” *Id.* at 25 (quoting Jakobsson Decl. ¶ 84). Petitioner corresponds Gardner’s network-based console to the claimed “security administrator device.” *Id.* According to Petitioner, it would have been obvious to combine Gardner’s administrator consoles with Gordon’s system “such that ‘authorized administrators’ could use the consoles to access data in ‘host monitoring system C’ over a network, as Gardner discloses.” *Id.* Moreover, Petitioner asserts, “[m]otivation to do so arises from the fact that Gardner describes the administrator consoles as an extension of the same ‘host monitoring system C’ that is in Gardner.” *Id.* at 26 (citing Ex. 1108 ¶ 57, Fig. 1; Ex. 1107, Fig. 5).

Patent Owner challenges Petitioner’s identification of Gardner’s consoles as the claimed “security administrator device.” PO Resp. 27–29. According to Patent Owner, “Gardner’s computer consoles do **not** manage the security of a security system.” *Id.* at 28. For reasons that follow, we do not agree with Patent Owner’s contention.

First, Patent Owner notes that Petitioner identified a different component in Gordon/Gardner combination for the claimed “security administrator device” in the ’595 IPR. PO Resp. 27. We agree with

Petitioner that this observation “is irrelevant.” Pet. Reply 24. As we stated in our Institution Decision, a petitioner may analyze a prior art reference differently in two different proceedings, including identifying different elements of the prior art with similar elements of different claims.

Institution Dec. 20–21. We therefore analyze the disclosure of the reference to determine whether it supports the Petitioner’s contentions in this proceeding.

Patent Owner contends Gardner’s computer consoles are not administrator devices because they “merely provide access to information through inputs and outputs,” and “are not devices that manage the security of a security system.” PO Resp. 29. We do not agree with Patent Owner’s argument because it is based on a construction of “security administrator device” that we did not adopt. *See* Section II.B.2, *supra*. Patent Owner’s construction would require “a device that manages the security of a security system.” PO Resp. 14 (emphasis omitted). Instead, we adopt Petitioner’s construction based on plain and ordinary meaning, which is “a device that performs security administration.” Pet. 14. Under our construction, Gardner’s console is a security administrator device because, as Petitioner notes, “it is used by ‘authorized administrators’ for the administrative purposes of accessing ‘location and asset related data.’” *Id.* at 25 (citing Ex. 1108 ¶¶ 59, 56, 60, 191).

We find that for the reasons given above, Petitioner demonstrates that the Gordon and Gardner teach element 1.2.a of claim 1.

d. Claim element 1.2.b

This claim element calls for “the mobile device including a mobile device processor and including a security agent configured to cooperate with

the security system.” Petitioner asserts Gordon includes a mobile device processor because its laptop has a “main processor.” Pet. 29 (quoting Ex. 1107, 11:28–29). Petitioner also asserts that together, Gordon’s security module 19 and host agent 14 “are a ‘security agent.’” *Id.* at 30. As Petitioner notes, “[t]hese two modules together being a ‘security agent’ is consistent with the ’632 patent embodiment where the security agent includes two modules—‘mode module 1904’ for waking components from a power management mode and ‘component manager 1906’ for conducting security services.” *Id.* (citing Ex. 1101, 28:11–20, 28:25–32, Fig. 19).

Patent Owner challenges Petitioner’s identification of the claimed “security agent” in Gordon. PO Resp. 24–27. According to Patent Owner, “Gordon’s host agent and security module (via its firmware agent), are capable of autonomous action, and they interact with other agents, namely each other.” *Id.* at 25. “Accordingly,” Patent Owner asserts, a skilled artisan “would not recognize Gordon’s host agent and security module to collectively make up the single ‘security agent.’” *Id.* at 26.

We disagree with Patent Owner’s argument. First, Patent Owner’s discussion about Gordon’s host agent and security module both being “capable of autonomous action” is irrelevant because it relies on Patent Owner’s construction of security agent that we declined to adopt for the reasons outlined in Section II.B.4, *supra*. In addition, we disagree with Patent Owner’s argument that Gordon’s host agent and security module cannot together be the claimed security agent because the claims do not restrict the security agent to a single module, and the specification discloses that the security agent may have multiple components. *See* Pet. Resp. 22. (citing Ex. 1101, Fig. 19).

In light of our construction of “agent,” *see* Section II.B.4, *supra*, a security agent need only be computer program designed to automate security tasks. We agree with Petitioner that together, Gordon’s security module 19 and host agent 14 “are a ‘security agent.’” Pet. 30; *see* Pet. Reply 21–24. We find that for the reasons given, Petitioner demonstrates that Gordon teaches element 1.2.b of claim 1.

e. Claim element 1.2.c

This claim element calls for “the security administrator device having a security administrator processor different than the mobile device processor, the mobile device being remote from the security administrator device.” Petitioner refers back to its analysis of element 1.2.a. Pet. 32. Petitioner contends “Gardner discloses that the ‘web-based or network based console’ computer (security administrator device) . . . is a different computer than at least certain of the host laptop devices disclosed in Gordon.” *Id.* (citing Ex. 1108 ¶ 57; Ex. 1107, 1:31–33). Petitioner also notes that because Gordon’s host laptops may be stolen, they are remote from the administrator’s computer console. *Id.* at 33 (citing Ex. 1107, 12:36–39, 13:30–34, 12:35–42, 14:53–60).

Other than as noted above, Patent Owner does not additionally challenge Petitioner’s showing for this element. *See* PO Resp. 39. We find that for the reasons given, Petitioner demonstrates that Gordon and Gardner teach element 1.2.c of claim 1.

f. Claim element 1.2.d

This claim element calls for “the mobile device being a first computer system, the security system being a second computer system, the security administrator device being a third computer system, the first computer

system, the second computer system and the third computer system being separate computer systems.” Petitioner asserts that Gordon and Gardner disclose this limitation because the host monitoring system (security system), laptop (mobile device), and administrator console (security administrator device) are all “discrete and separate” systems.” Pet. 33–34.

Patent Owner does not challenge Petitioner’s showing for this element. We find that for the reasons given, Petitioner demonstrates that Gordon and Gardner teach element 1.2.d of claim 1.

g. Claim elements 1.3 and 1.4.a

These claim elements, together, call for “a security system processor being different than the mobile device processor and different than the security administrator processor, the security system processor being configured to store in the security system memory at least a portion of wake code, the wake code being configured to detect a wake event and to send a wake signal to the mobile device in response to detecting the wake event.”

Petitioner asserts Gordon’s host monitoring system C / monitoring center 70 (a security system) “necessarily and inherently includes a processor,” Pet. 34, 35, that is separate from the processors in Gordon’s laptop and Gardner’s console, *id.* at 35. Petitioner explains that Gordon’s monitoring center 70 (the claimed security system) includes the claimed “wake code” that “detect[s] a wake event” because Gardner describes that “the monitoring center may . . . indicate that the firmware agent should wake-up the host.” *Id.* at 35–36 (quoting Ex. 1107, 4:58–63). Gordon discloses that the monitoring center 70 sends wake signals in response to detected wake events (as the challenged claims require) because “the monitoring center may send a wake signal if it receives a response to a call

from the laptop's firmware agent 21 instead of the host agent 14.” *Id.* at 36 (citing Ex. 1107, 16:23–17:9, Fig. 4). “In this scenario,” Petitioner explains, “the receipt of the return call from the firmware agent would be a detected wake event because it triggered the monitoring center to send a wake-up signal.” *Id.* at 36–37.

Other than as explained above, Patent Owner does not separately challenge Petitioner's arguments for these elements. We find that for the reasons given, Petitioner demonstrates that Gordon and Gardner teach elements 1.3 and 1.4.a.

h. Claim element 1.4.b

This claim element calls for “the security agent of the mobile device being configured to receive the wake signal, the security agent of the mobile device being configured to wake at least a portion of the mobile device from a power management mode in response to receiving the wake signal, the security agent of the mobile device being configured to perform security services after the at least a portion of the mobile device has been woken.”

Petitioner contends Gordon discloses this element because Security module 19 and its firmware agent 21 receives the wake signals and in response, security module 19 wakes part of the laptop from a power management mode (i.e. low power, sleep or shut-down modes). Pet. 39–40. In particular, Petitioner explains, security module 19 and its firmware agent 21 wakes up host agent 14, which then performs security services (e.g., deleting data, protecting data, updating software, and deploying software) after a portion of the mobile device has been woken.” Pet. 40–41 (citing Ex. 1107).

Other than as outlined above, Patent Owner does not additionally challenge Petitioner's showing for this element. We find that for the reasons given, Petitioner demonstrates that Gordon teaches element 1.4.b of claim 1.

i. Claim elements 1.5, 1.6, 1.7.a, and 1.7.b

These claims elements call for the following:

[1.5] detect a particular wake event;

[1.6] prepare a particular wake signal in response to detecting the particular wake event; and

[1.7.a] send the particular wake signal to the mobile device in response to detecting the particular wake event,

[1.7.b] the security agent of the mobile device being configured to wake the at least a portion of the mobile device in response to receiving the particular wake signal and being configured to perform particular security services after the at least a portion of the mobile device has been woken.

Petitioner demonstrates that each of these limitations is disclosed by Gordon. Pet. 42–44. Petitioner refers back to its analysis of claim element 1.4.a, describing the Gordon's wake event and signal. *Id.* at 42–43.

Petitioner points out that Gordon's security system (monitoring center 70 / host monitoring system C) detects "particular" wake events distinguishable from other wake events, such as those that happen at other times. *Id.* at 42; *see* discussion of "particular" wake events and signals in Section II.B.3, *supra*. Moreover, Gordon discloses performing particular security services after a portion of the mobile device has been woken because "Gordon discloses that the laptop's security module 19 and its firmware agent 21 (part of the 'security agent') may receive wake signals to 'wake-up the host so

that a data protection measure can be invoked.” *Id.* at 44 (quoting Ex. 1107, 4:58–63).

Patent Owner characterizes the “alleged” wake signal in Gordon as flawed because “because the same message is sent whether or not the computer and/or host agent is active.” PO Resp. 22. We disagree with this argument because “a prior art product that sometimes, but not always, embodies a claimed method nonetheless teaches that aspect of the invention.” *Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1326 (Fed. Cir. 2003). As Petitioner notes, Gordon discloses that “[t]he call may involve, for example, an instruction to the firmware agent to switch on the computer and/or wake up the host agent.” Pet. Resp. 17 (quoting Ex. 1107, 17:7–9). It does not matter that Gordon’s also discloses messages that are not wake calls because the host is already active.

Patent Owner also contends that Gordon’s message is insufficient because “it is a generic wake signal, not a particular one.” PO Resp. 22. This is a variation on Patent Owner’s argument that the claims require a particular “type” of wake event or wake signal, which we rejected as contrary to the language of the claims. *See* Section II.B.3, *supra*. We find that Gordon’s SMS call is a particular wake signal because it is distinguishable from other wake signals on the basis of the time it was sent. Pet. Reply 15.

Moreover, even under Patent Owner’s construction of “particular,” which we have not adopted, Gordon discloses a “a particular type of wake signal” because “Gordon discloses that the SMS call may include ‘an instruction to the firmware agent to switch on the computer and/or wake up the host agent.’” Pet. Resp. 16 (quoting Ex. 1107, 17:7–9). As Petitioner

explains, “[t]his passage discloses three particular types of wake signals: 1) one with an instruction to switch on the computer; 2) one with an instruction to wake up the host agent; 3) one with an instruction to do both.” *Id.* at 16.

We find that for the reasons given, Petitioner demonstrates that asserted prior art teaches elements 1.5, 1.6, 17.a.1, and 17.a.2 of claim 1.

j. Summary

We have considered Petitioner’s analysis of claim 1 in relation to the asserted prior art and the relevant arguments and evidence presented by Patent Owner. Considering the entire record, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 1 of the ’632 patent would have been obvious in light of Gordon and Gardner.

2. Claim 16

Claim 16 is directed to “[a] non-transitory computer readable medium in a security system,” but is otherwise similar to claim 1. Petitioner’s analysis of claim 16 relies on its analysis of claim 1. Pet. 46–48. Patent Owner does not address claim 16 separately, but combines its analysis of common elements in claim 16 with its analysis of claim 1. *See* PO Resp. 19–29. Considering the entire record, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 16 of the ’632 patent would have been obvious in light of Gordon and Gardner for the reasons given for claim 1.

3. Claims 7 and 22

Claims 7 and 22 depend from claim 1 and claim 16, respectively, each adding the limitation “wherein the wake event includes at least detecting a predetermined clock time.” wherein the performing the particular security services includes removing unauthorized data from the

mobile device.” Petitioner asserts Gordon discloses this limitation because “Gordon discloses that the laptop host device (a mobile device) may call the monitoring center (a security system) at predetermined times, such as every 15 minutes.” Pet. 44 (citing Ex. 1107, 15:17–18, 16:60–61); *see id.* at 45, 49. Other than the arguments explained above, Patent Owner does not additionally contest claims 7 and 22. For the reasons given, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 7 and 22 would have been obvious in light of Gordon and Gardner.

4. Claims 9 and 24

Claims 9 and 24 depend from claim 1 and claim 16, respectively, each adding the limitation “wherein the performing the particular security services includes removing unauthorized data from the mobile device.” Petitioner asserts Gordon teaches this limitation because “Gordon discloses that the services invoked by the security module 19 on a laptop include ‘data delete.’” Pet. 45 (citing Ex. 1107, 3:43–45, 7:33–42). Petitioner further explains, with support from its expert, that “[a skilled artisan] would have understood that this ‘data delete’ process refers to removing unauthorized data because as soon as an administrator or user has determined that certain data should be deleted, that data is no longer authorized to be on the mobile device.” *Id.* (citing Jakobsson Decl. ¶ 132). Other than the arguments explained above, Patent Owner does not additionally contest claims 9 and 24. For the reasons given, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 9 and 24 would have been obvious in light of Gordon and Gardner.

B. ADDITIONAL GROUNDS FOR CLAIMS 7, 9, 22, AND 24

Petitioner contends claims 7 and 22 would have been obvious over Gordon, Gardner, and Chang. Petitioner’s challenge mirrors its earlier challenge to these claims based on Gordon and Gardner, except Petitioner relies on Chang for teaching the additional limitation in claim 7 and 22 of “a wake event that includes detecting a predetermined clock time.” Pet. 52, 55. According to Petitioner, “[a person of ordinary skill] could implement a Gordon wake signal to be sent in 15 minutes from the present time (a predetermined clock time) or at any other predetermined time in the future, as described by Chang.” *Id.* at 53–54. Petitioner explains that a skilled artisan would have been motivated to combine the references based on “Chang’s teaching that it would be desirable to send wake signals to computers at certain predetermined clock times.” *Id.* at 54 (citing Ex. 1110 ¶ 4). Patent Owner’s response does not additionally challenge Petitioner’s alternative grounds for claims 7 and 22. For the reasons given, we find that Petitioner has demonstrated that claims 7 and 22 would have been obvious over Gordon, Gardner, and Chang.

Petitioner further contends claims 9 and 24 would have been obvious over Gordon, Gardner, and Meenan. Petitioner’s challenge mirrors its earlier challenge to these claims based on Gordon and Gardner, except Petitioner relies on Meenan for teaching the additional limitation in claim 9 and 24 of “wherein the performing the particular security services includes removing unauthorized data from the mobile device.” Pet. 56, 60. According to Petitioner, Meenan teaches “a scanner application . . . to detect and remedy ‘unauthorized programs.’” *Id.* at 57 (citing Ex. 1111 ¶¶ 16–21, 26, 32, Figs. 1, 2). A skilled artisan would have been motivated to combine

the references as Petitioner proposes “to secure a computer by removing unauthorized programs from it, as disclosed by Meenan.” *Id.* at 59 (citing Ex. 1111 ¶ 57). Patent Owner’s response does not additionally challenge Petitioner’s alternative grounds for claims 9 and 24. For the reasons given, we find that Petitioner has demonstrated that claims 9 and 24 would have been obvious over Gordon, Gardner, and Meenan.

IV. CONCLUSION

For the foregoing reasons, we determine Petitioner has demonstrated by a preponderance of the evidence that all challenged claims of the ’632 patent would have been obvious and are, therefore, unpatentable. Our conclusions are summarized in the following table.

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1, 7, 9, 16, 22, 24	103(a)	Gordon, Gardner	1, 7, 9, 16, 22, 24	
7, 22	103(a)	Gordon, Gardner, Chang	7, 22	
9, 24	103(a)	Gordon, Gardner, Meenan	9, 24	
Overall Outcome			1, 7, 9, 16, 22, 24	

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1, 7, 9, 16, 22, and 24 of the ’632 patent are unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

James Heintz
Michael Burns
Robert Buergi
Jennifer Nall
DLA Piper LLP (US)
jim.heintz@dlapiper.com
michael.burns@dlapiper.com
robert.buergi@dlapiper.com
jennifer.nall@us.dlapiper.com

PATENT OWNER:

Jonathan Caplan
Jeffrey Price
KRAMER LEVIN NAFTALIS &
FRANKEL LLP
jcaplan@kramerlevin.com
jprice@kramerlevin.com