Trials@uspto.gov
571-272-7822

Paper 13
Date: May 6, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

CROWDSTRIKE, INC.,
Petitioner,

v.

GOSECURE, INC.,
Patent Owner.

---

IPR2025-00067
Patent 9,106,697 B2

---

Before NEIL T. POWELL, STACEY G. WHITE, and GARTH D. BAER, *Administrative Patent Judges*.

BAER, *Administrative Patent Judge*.

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

# I. INTRODUCTION

## *A. Background and Summary*

CrowdStrike, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–23 ("challenged claims") of U.S. Patent No. 9,106,697 B2 (Ex. 1001, "the '697 patent"). GoSecure, Inc. ("Patent Owner") filed a statutory disclaimer of claims 19 and 20 (Ex. 2010) and a Preliminary Response (Paper 7, "Prelim. Resp."). With our authorization, Petitioner filed a Reply to Patent Owner's Preliminary Response (Paper 9, "Reply") and Patent Owner filed a Preliminary Sur-reply (Paper 10, "Sur-reply").

Under 35 U.S.C. § 314, an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Upon consideration of the Petition in view of the present record and for the reasons explained below, we determine that Petitioner has not shown a reasonable likelihood of prevailing with respect to at least one of the challenged claims. Accordingly, we do not institute an *inter partes* review on the grounds set forth in the Petition. *See* 37 C.F.R. § 42.108(a).

## *B. Related Proceedings*

The parties identify the following related matter: *GoSecure Inc. v. CrowdStrike, Inc., and CrowdStrike Holdings, Inc.*, No. 24-cv-526 (W.D. Tex.). Pet. 83; Paper 5, 1. The '697 patent is also the challenged patent in IPR2025-00069.

## *C. The '697 Patent*

The '697 patent relates to "analyzing malicious activities on a computer system in order to better protect the computer system from future malicious activity." Ex. 1001, 1:33–36. The patent describes using a virtual

machine as a decoy computer system to monitor for unauthorized activities and generating a fingerprint indicative of those unauthorized activities, which can then be used to protect the remainder of the computer network against similar unauthorized activities. *Id.* at 1:44–46, 2:9–12, 2:26–36, 4:43–46. Figure 2 of the '697 patent is reproduced below.

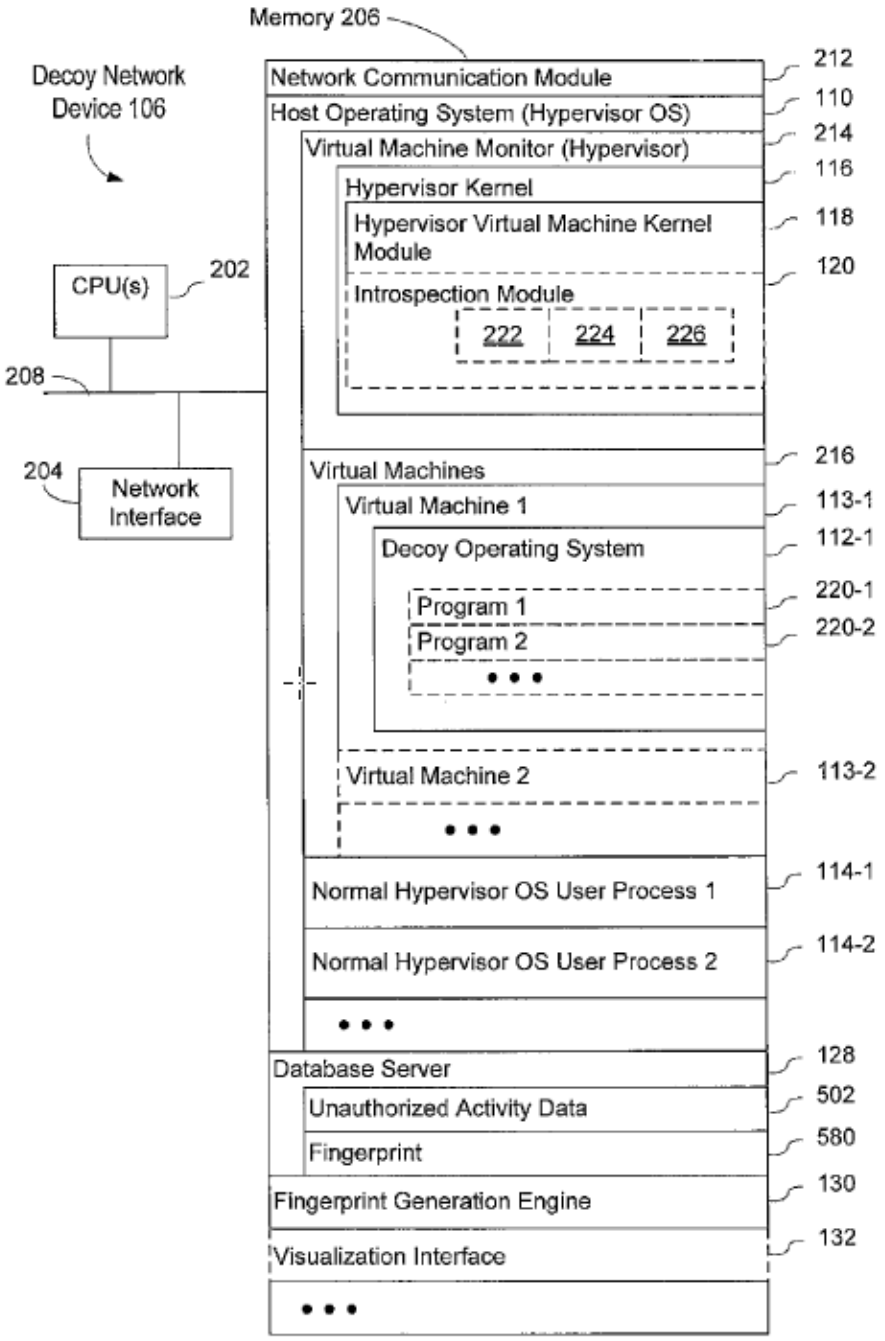


**Figure 2**

Figure 2 "is a block diagram illustrating the decoy network device." *Id.* at 3:19–20.

*D. Statutory Disclaimer and Remaining Challenged Claims*

The Petition challenges claims 1–23. Pet. 8. However, because Patent Owner disclaimed claims 19 and 20 (Ex. 2010), the remaining challenged claims are 1–18 and 20–23. *See* 37 C.F.R. § 42.107(e) (2020) ("No *inter partes* review will be instituted based on disclaimed claims."). Of the remaining challenged claims, only claim 1 is independent. Claim 1 is reproduced below:

> 1. A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises:
>
> one or more processors; and
>
> memory storing:
>
> a virtual machine; and
>
> a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:
>
> monitoring activity on the virtual machine;
>
> identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
>
> storing in the memory the activity sources, activity targets, and associations;
>
> creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and
>
> transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

Ex. 1001, 19:2–25.

*E. Prior Art and Asserted Grounds*

Petitioner asserts the following grounds of unpatentability:

| Claim(s) Challenged | 35 U.S.C. §[1] | References/Basis |
|---|---|---|
| 1–13, 15–17, 19–23 | 103 | Capalik,[2] King[3] |
| 14 | 103 | Capalik, King, Pike[4] |
| 18 | 103 | Capalik, King, Farley[5] |

Pet. 8.

## II. DISCUSSION

*A. Level of Ordinary Skill in the Art*

Petitioner contends a person of ordinary skill in the art at the time of the invention would have "a bachelor's degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience" and "a working knowledge of software security analysis and dynamic malware analysis." Pet. 7. Further, "[a]dditional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education." *Id*. Patent Owner does not challenge Petitioner's definition at this stage of the proceeding. Prelim. Resp. 13. On this record, we agree with Petitioner's definition.

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), included revisions to 35 U.S.C. § 103 that became effective after the filing of the application that led to the challenged patent.
[2] US 2008/0016570 A1, Pub. Jan. 17, 2008 (Ex. 1004, "Capalik").
[3] Samuel T. King, "*Analyzing Intrusions Using Operating System Level Information Flow*," Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in The University of Michigan, 2006 (Ex. 1006, "King").
[4] US 8,819,822 B1, Aug. 26, 2014 (Ex. 1007, "Pike").
[5] US 7,089,428 B2, Aug. 8, 2006 (Ex. 1008, "Farley").

*B. Description of Primary Prior Art Reference*

*1. Capalik (Ex. 1004)*

Capalik "relates to the field of methods and systems for protecting computer networks." Ex. 1004 ¶ 2. Capalik's Figure 5 is reproduced below.

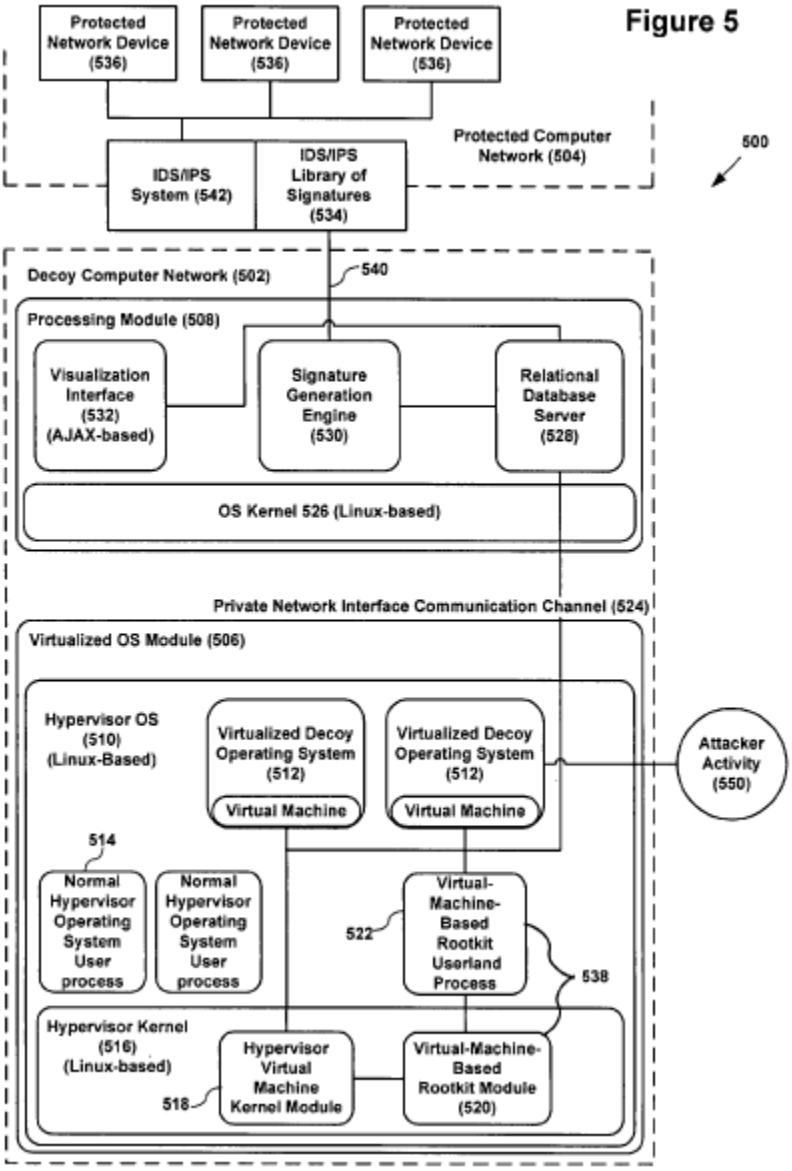


Figure 5 is a block diagram showing "a system for analyzing and preventing unauthorized intrusion into a computer network." Ex. 1004 ¶¶ 20, 37. "In use, attacker activity 550 is directed at the decoy computer network 502 through one more ports . . . that are left open as a gateway for attacker

activity." *Id.* ¶ 44. When an attacker connects to an open port, decoy computer network 502 "monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, ASCII or binary files, malicious payloads, memory manipulation attempts, and any other data transfers or malicious attempts." *Id.* ¶ 49. If the interaction warrants creating an attack signature, decoy computer network 502's processing module 508 may generate an attack signature. *Id.* ¶¶ 52, 59.

*2. King (Ex. 1006)*

King teaches methods for analyzing unauthorized intrusions into computer systems. Ex. 1006, 2–3. King teaches various tools that identify, store, and display information about unauthorized intrusion events. *See, e.g.*, *id.* at 12 (describing "*EventLogger* which logs information-flow events in real time" and "*GraphGen* that processes EventLogger logs to generate the information-flow graphs we use to analyze intrusions"); *id.* at 13–14.

*C. Obviousness Analysis*

*1. Petitioner's Proposed Prior-Art Combination*

In challenging claims 1–23, Petitioner relies primarily on Capalik and King. *See* Pet. 19–79.[6] Petitioner explains that Capalik teaches the claimed decoy computer system (decoy computer network 502) and a "introspection module 538 [that] monitors and captures attack-identifying information, which is stored as forensic data for later analysis." *Id.* at 10–11 (citing Ex. 1004 ¶¶ 38, 49–52). Capalik also teaches that "[s]ignature generation engine

[6] Petitioner adds Pike for teaching the additional limitation in dependent claim 4 (identifying attempts to access non-executable memory) and Farley for teaching the additional limitation in dependent claim 18 (determining a frequency of unauthorized activities). *Id*. at 71–79.

530 uses . . . forensic data to generate an attack signature." *Id.* at 11 (citing Ex. 1004 ¶ 52). Petitioner explains that in Capalik's system, "[t]he attack signature is then sent to the IDS/IPS system 542, which uses the signature to identify and prevent subsequent attacks." *Id.* (citing Ex. 1004 ¶ 54). Petitioner asserts that a skilled artisan would have modified Capalik's system "to include King's teachings to identify, store, and graphically display attack activities including the activity sources, activity targets, and associations between them" to provide security improvements because "gathering more detailed threat information provides improved threat analysis." *Id*. at 38 (citing Ex. 1003 ¶ 131).

*2. "creating . . . a fingerprint"*

Claim 1 requires a decoy system that comprises a virtual machine and "at the virtual machine monitor: . . . creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine." Ex. 1001, 19:4–22. Petitioner asserts that Capalik teaches the claimed fingerprint creation because "Capalik discloses decoy system processing module 508 generates an attack report containing attack-identifying information." Pet. 45 (citing Ex. 1004 ¶ 55). Patent Owner argues that Petitioner's challenge fails because claim 1 "plainly requires the virtual machine monitor to be involved in creating a fingerprint," yet "fingerprint generation in Capalik occurs entirely ***outside*** the virtual machine monitor." Prelim. Resp. 21–22. As outlined below, we agree with Patent Owner.

Petitioner does not contest that Capalik's fingerprint generation occurs outside the components that Petitioner identifies as the claimed virtual machine monitor. Reply 1–3; *see* Pet. 24–26, 41–47 (mapping Capalik's hypervisor kernel 516 to the claimed virtual machine monitor and signature generation engine 530 to the claimed fingerprint creation); Prelim. Resp. 22–

25 (explaining Petitioner's mapping). Instead, Petitioner asserts that the at-issue claim language—"at the virtual machine monitor"—does not require "that each of the subsequently recited steps must be performed ***by or in*** the [virtual machine monitor]," but instead only requires "that the fingerprint is generated by the same decoy system that contains the [virtual machine monitor]." Reply 2. Petitioner argues that the intrinsic record supports its position because "[n]owhere in the '697 Patent is there any teaching or suggestion that a [virtual machine monitor] creates a fingerprint/signature indicative of attack activity," and instead, "[t]he '697 Patent teaches that its signature generation engine is separate from the [virtual machine monitor]." Reply 2 (citing Ex. 1001, Fig. 2). In addition, Petitioner asserts that requiring fingerprint creation at the virtual machine monitor "directly conflicts with the broader interpretation [Patent Owner] has advanced in parallel litigation." *Id.* at 3 (citing Ex. 1027).

We disagree with Petitioner's arguments. Claim 1 recites "a decoy computer system [that] comprises . . . a virtual machine monitor," and "at the virtual machine monitor: . . . creating, from the stored activities, a fingerprint." Ex. 1001, 19:4–22. Thus, the claim's plain language requires creating a fingerprint at the virtual machine monitor, not just at the decoy system, as Petitioner asserts. When, as here, a claim term has "ordinary, simple English words whose meaning is clear and unquestionable," we may not redraft those words to mean something different. *Chef America, Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1373–75 (Fed. Cir. 2004). Petitioner offers no explanation how one skilled in the art might read "at the virtual machine monitor" to mean at the decoy system, rather than at the virtual machine monitor. Although the claim's plain language is decisive, we also disagree with Petitioner's assertion that the '697 patent's specification

describes only fingerprint creation outside the virtual machine monitor because, as Patent Owner explains, the specification describes fingerprint generation inside and outside the virtual machine monitor. Sur-reply 1–2; *see id.* at 2 (citing Ex. 1001, 6:65–7:2, 10:13–22). Claim 1's plain language, however, only covers the latter. Sur-reply 1–2; *see id.* at 2 (citing Ex. 1001, 6:65–7:2, 10:13–22). Last, Petitioner's characterization of Patent Owner's infringement allegations in the related district-court proceedings, even if correct, do not undermine the claim's plain language.

Given the deficiencies outlined above, Petitioner has not shown that the prior art teaches or suggests creating a fingerprint at the virtual machine monitor as the challenged claims require. Thus, Petitioner has not shown a reasonable likelihood of prevailing with respect to at least one of the challenged claims.

## III. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has not demonstrated a reasonable likelihood of success in proving that at least one of the challenged claims of the '697 patent is unpatentable. We therefore do not institute trial on any challenged claims or grounds raised in the Petition.

## IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), no *inter partes* review is instituted for claims 1–23 of the '697 patent on the unpatentability grounds asserted in the Petition.

PETITIONER:

Paul Hart
Adam Seitz
ERISE IP, P.A.
paul.hart@eriseip.com
adam.seitz@eriseip.com

PATENT OWNER:

Srinivas Giriraj Pathmanaban
Raghav Bajaj
Daniel Todd
Steven Peters
LATHAM & WATKINS LLP
gpathmanaban@cgsh.com
raghav.bajaj@lw.com
daniel.todd@lw.com
steven.peters@lw.com