



ORAL ARGUMENT FOR IPR2024-00332 (10,929,512) & IPR2024-00334 (11,514,138)

Before Administrative Patent Judges

- Jameson Lee
- Arthur Peslak
- Steven Amundson

Summary

The 512 Patent

1. The Art Does Not Render Obvious the Claims:

- Kesanupalli in light of Challenger and Cheng does not teach or render obvious a second processor configured to *perform* a secure backup of the record to a storage service or cloud storage.

2. Apple's Improper Broadening of Claims:

- Apple improperly relies on unclaimed embodiments to broaden the term *perform*.

3. Late Claim Construction Arguments:

- Apple did not seek to broadly construe *perform* and has waived its argument.

The 512 and 138 Patents

1. A POSITA Would Not Have Combined Kesanupalli with Challenger:

- A POSITA would not have added Challenger's TPM to Kesanupalli's system.

The 138 Patent

1. A POSITA Would Not Have Combined Kesanupalli with Brown:

- A POSITA would not have added Brown's wiping capabilities to Kesanupalli's system.

The 512 Patent Is Patentable

Patentable Over Apple's Prior Art

Apple's prior art does not render obvious the claims' "second processor is configured to . . . perform a secure backup of the record to a storage service" (claims 1/11/21) and "wherein the storage service comprises ad cloud storage service" (claims 2/12) limitations

Summary

The 512 Patent

1. The Art Does Not Render Obvious the Claims

- Kesanupalli in light of Challenger and Cheng does not teach or render obvious a second processor configured to *perform* a secure backup of the record to a storage service or cloud storage.

2. Apple's Improper Broadening of Claims:

- Apple improperly relies on unclaimed embodiments to broaden the term *perform*.

3. Late Claim Construction Arguments:

- Apple did not seek to broadly construe *perform* and has waived its argument.

The 512 and 138 Patents

1. A POSITA Would Not Have Combined Kesanupalli with Challenger:

- A POSITA would not have added Challenger's TPM to Kesanupalli's system.

The 138 Patent

1. A POSITA Would Not Have Combined Kesanupalli with Brown:

- A POSITA would not have added Brown's wiping capabilities to Kesanupalli's system.

The Board Must Consider The Precise Words Of The Claims



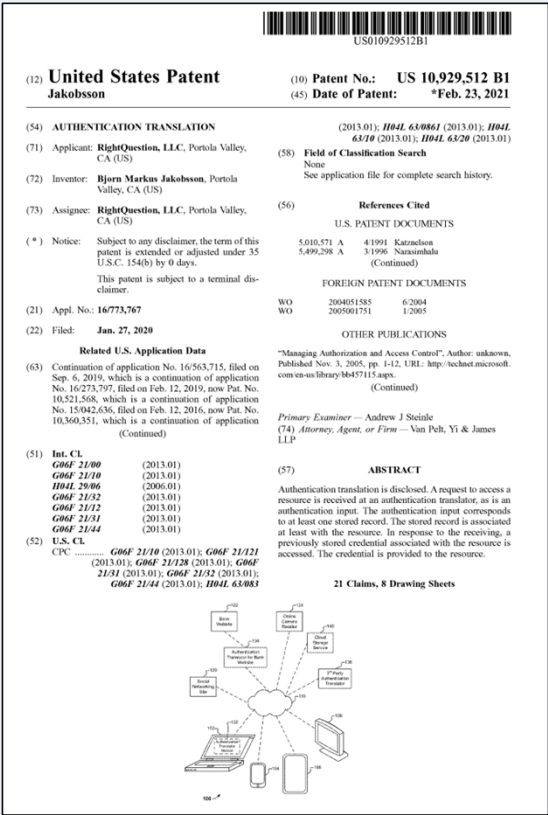
“To determine the latter—what exactly was claimed—the focus is on the precise words of the particular claim or claims at issue.”

MySpace, Inc. v. GraphOn Corp., 672 F.3d 1250, 1256 (Fed. Cir. 2012)

“After all, the claims, not the specification, provide the measure of the patentee’s right to exclude.”

Johnson & Johnston Associates Inc. v. R.E. Service Co., Inc., 285 F.3d 1046, 1053 (Fed. Cir. 2002) (en banc).

The Claim Language Is Clear: The Second Processor Must Perform The Secure Backup To A Storage Service



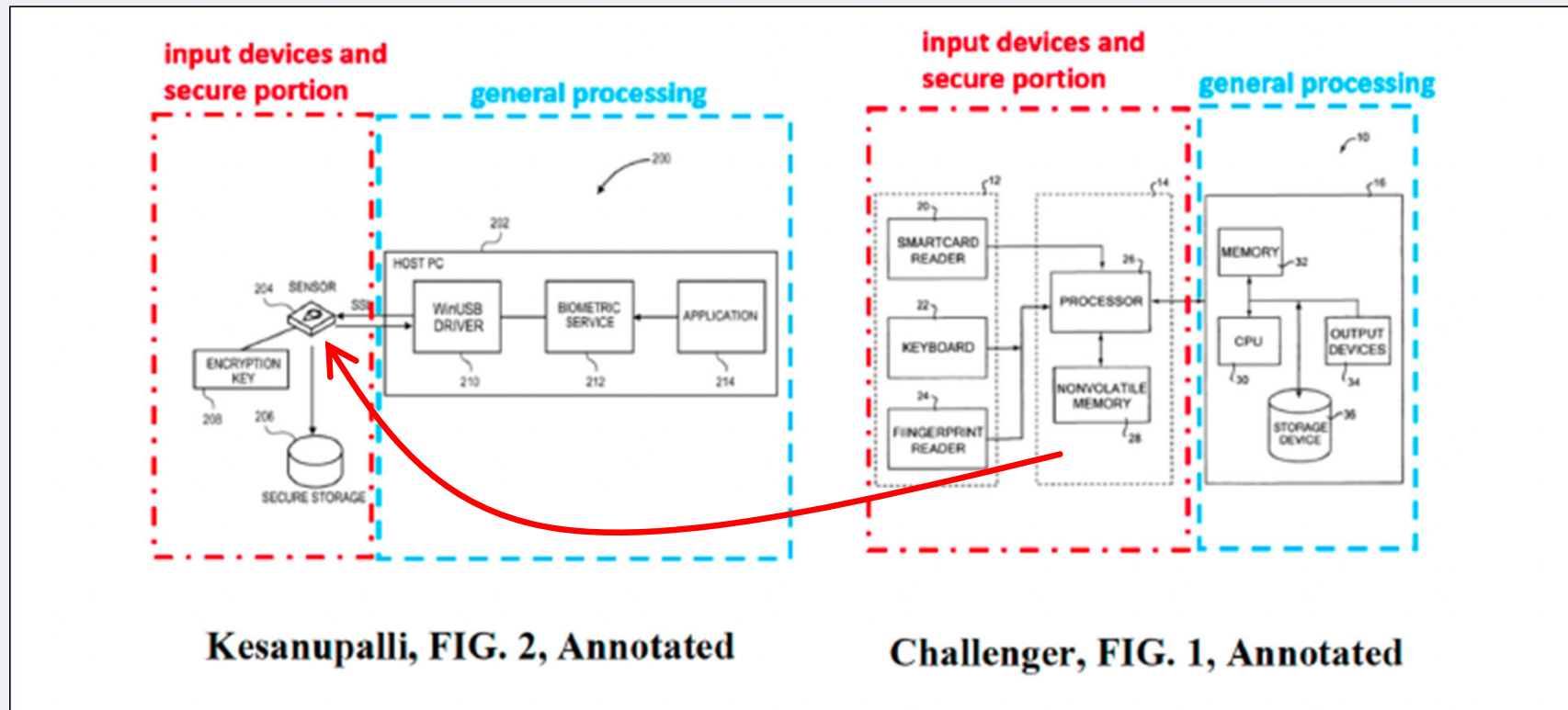
1. A system, comprising:
a first processor of a first device, wherein the first processor is configured to:

...
communicate with a second processor using a restricted interface, wherein the second processor is configured to:

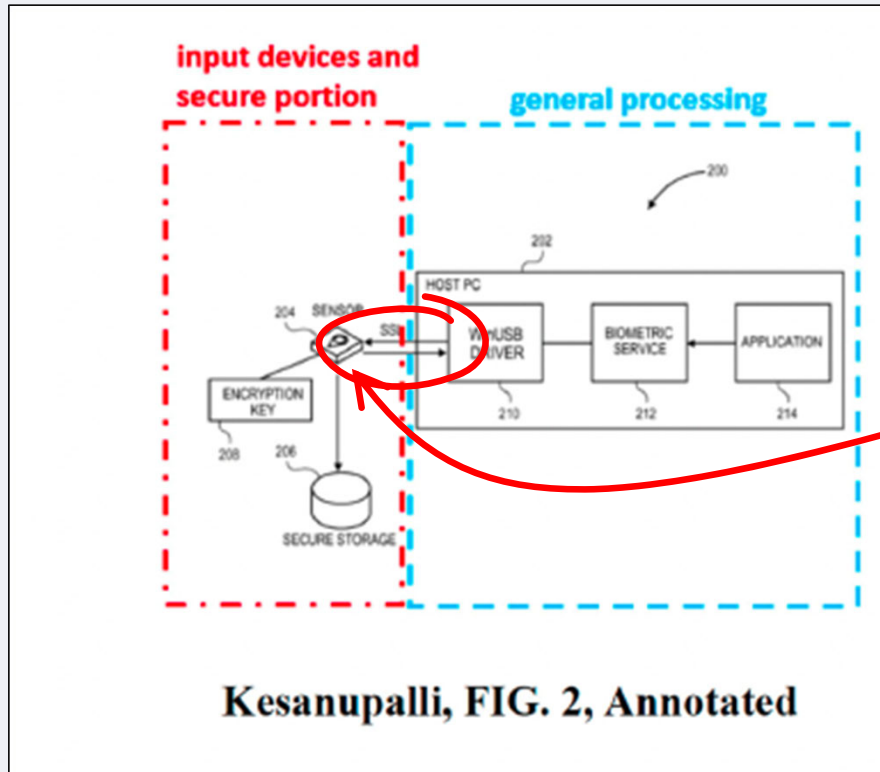
...
perform a secure backup of the record to a storage service, wherein a second device associated with the user is registered with the storage service, and wherein the record is downloaded from the storage service by the second device; and

...

Kesanupalli In Light Of Challenger and Cheng Does Not Teach A “Second Processor [] Configured To . . . Perform A Secure Backup Of The Record To A Storage Service” (Claims 1/11/21) And “Wherein The Storage Service Comprises A Cloud Storage Service” (Claims 2/12)



The Sensor Processor/TPM (Alleged Second Processor) Communicates With The General Processor (Alleged First Processor) Only



The Sensor Processor/TPM can only communicate with the general processing of the system.

The Sensor Processor/TPM (the alleged second processor) does not perform the backup to a storage service (claim 1) or cloud storage (claim 2) by handing the backup off to the general processing section (the alleged first processor).

Dr. Goodrich: In The Kesanupalli/Challener/Cheng Architecture, The “General Processor Would . . . Be The Processor That Actually Performs The Backup To A Storage Service.”

66. . . . Petitioner alleges the combination of a secure portion and sensor is the second processor, which must “perform a secure backup of the record to a storage service.” Petition at 21. **However, the TPM and sensor combination are not isolated and are not connected to any storage service. The TPM and sensor combination can only communicate with the general processor.** This general processor would be the processor that actually performs a backup to a storage service. . .

67. Cheng cannot remedy this architectural deficiency, which does not meet the '512 Patent's claim language. Further combining the Cheng reference does not change what can access the Kesanupalli reference's secure portion. *See, e.g.,*

Petition at 38 (“Such restrictions limit access and thereby protect the functions and data in the security portion of a TPM-based security architecture (e.g., sensor 204 and the secure storage 206) from being misused by an untrusted or malicious program.”). **Cheng does not change that the sole connection between the sensor (which is combined with a TPM) and Host PC 202 is an SSL connection.** Ex. 1006 at 6:39-41, Figs. 1-2. Combining the Cheng reference with the Kesanupalli and Challener references does not change that the general processor – as opposed to the TPM and sensor combination – would be the processor that actually performs a backup to a storage service. . .

IPR2024-00332, Ex. 2037 (Goodrich 512 Decl.) at ¶¶ 66-67

IPR2024-00332, 512 PO Response at 32-34

IPR2024-00332, PO Sur-Reply at 2-4

Demonstrative Exhibit - Not Evidence

Apple Ignores The Claim Language

Apple Position

- The specification shows that the second processor need not perform all the steps of the backup in order to *perform* the backup.

Carbyne Response

- The claim language makes clear that the second processor must perform the backup and not just initiate or facilitate the backup.
- It's improper to read the embodiments into the specification to broaden the claims.
- Apple's claim construction arguments are too late.

IPR2024-00332, 512 PO Response at 31-35

IPR2024-00332, PO Sur-Reply at 4-8

IPR2024-00332, Pet. Reply at 21-24

Apple Conflates Perform and Facilitate



“There is an inference . . . that two different terms used in a patent have different meanings.”

Comaper Corp. v. Antec, Inc., 596 F.3d 1343, 1348 (Fed. Cir. 2010)

Apple Conflates Perform and Facilitate

512 Patent	Petitioner's Understanding of the 512 Patent
communicate with a second processor using a restricted interface, wherein the second processor is configured to: ... in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor, facilitate a login of the user to the external resource at least in part by transmitting ... perform a secure backup of the record to a storage service . . .	communicate with a second processor using a restricted interface, wherein the second processor is configured to: ... in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor, facilitate a login of the user to the external resource at least in part by transmitting ... facilitate a secure backup of the record to a storage service . . .

IPR2024-00332, Exhibit 1001 - Patent
IPR2024-00332, PO Sur-Reply at 6-7

Dr. Goodrich: Apple's Apparent Understanding of the Claim, Conflates Perform and Facilitate

69. Limitation 1.6B merely requires that the second processor **facilitate** a login that either the first processor or the second processor can complete. In contrast, Limitation 1.7A requires that the second processor **perform** a secure backup of the record to a storage service. Limitation 1.7A is not met if the first processor performs or completes the performance of a secure backup of the record to a storage service. The TPM and sensor combination is not a second processor that performs a secure backup of the record to a storage service.

IPR2024-00332, Ex. 2037 (Goodrich 512 Decl.) ¶ 69

Apple Reads Unclaimed Embodiments Into The Claims

Apple Position

- “PO’s attempt to characterize the second processor as performing the secure backup without any communication with the first processor is in conflict with its own patent’s disclosure.”

Carbyne Response

- Not all embodiments have to be claimed.
- US Patent 11,475,105—which shares a specification with the ’512 Patent— claims a processor configured to “initiate a backup.”

IPR2024-00332, 512 Pet. Reply at 21-24
IPR2024-00332, 512 PO Sur-Reply at 4-6
IPR2024-00332, Ex. 2028 (105 Patent) at claim 1

Dr. Goodrich Did Not Admit That The Claims Must Practice The Embodiment As Apple Suggests

Apple
Position

- “PO’s expert agrees that the communication flow is between the second processor and the first processor”

Dr. Goodrich
Deposition

- “***So figure 3 is an illustration of an embodiment*** of a device which secures storage.”
- “If you're asking about the ***preferred embodiment*** of how -- what figure 3 is illustrating,¹⁰ that's discussed, for example, beginning in column 3,¹¹ starting at line 66, and then continuing into 12 column 4.”
- “Yes, because if we look just to the part 20 before that, it says, beginning at line 66 of 21 column 3, ‘***one example*** of a device with secure 22 storage is illustrated in figure 3.”

Carbyne
Response

- Dr. Goodrich was asked about certain embodiments where there is a communication flow between the *second processor* and the *first processor*.
- Dr. Goodrich never stated that was the only way or that it was required by the claims

IPR2024-00332, 512 Pet. Reply at 22-23 .
IPR2024-00332, Ex. 1031 (Goodrich Depo.) at 35-36.
IPR2024-00332, 512 PO Sur-Reply at 5-6.

Apple Waived It's Claim Construction Arguments

“In addition to the requirements of §§ 42.6, 42.8, 42.22, and 42.24, the petition must set forth: . . . How the challenged claim is to be construed.”

37 C.F.R. § 42.104(b)(3)

The 512 and 138 Patents Are Patentable Over The Art

Petitioner Has Failed To Show A POSITA Would Have Been Motivated To Modify Kesanupalli in
Light of Challenger

Summary

The 512 Patent

1. The Art Does Not Render Obvious the Claims:

- Kesanupalli in light of Challenger and Cheng does not teach or render obvious a second processor configured to *perform* a secure backup of the record to a storage service or cloud storage.

2. Apple's Improper Broadening of Claims:

- Apple improperly relies on unclaimed embodiments to broaden the term *perform*.

3. Late Claim Construction Arguments:

- Apple did not seek to broadly construe *perform* and has waived its argument.

The 512 and 138 Patents

1. A POSITA Would Not Have Combined Kesanupalli with Challenger:

- A POSITA would not have added Challenger's TPM to Kesanupalli's system.

The 138 Patent

1. A POSITA Would Not Have Combined Kesanupalli with Brown:

- A POSITA would not have added Brown's wiping capabilities to Kesanupalli's system.

Grounds Including The Kesanupalli and Challenger Combination

IPR Proceeding	Grounds
IPR2024-00332 (512)	All Grounds
IPR2024-00334 (138)	Ground 3

IPR2024-00332, 512 PO Sur-Reply at 8-9
IPR2024-00334, 138 PO Sur-Reply at 1-4

The Board Must Consider The Art For All It Teaches



“It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art.”

In re Wesslau, 353 F.2d 238 (CCPA 1965)

“Evidence suggesting reasons to combine cannot be viewed in a vacuum apart from evidence suggesting reasons not to combine”

Arctic Cat Inc. v. Bombardier Recreational Prods. Inc., 876 F.3d 1350, 1363 (Fed. Cir. 2017)

IPR2024-00332, 512 PO Sur-Reply at 8-9
IPR2024-00334, 138 PO Sur-Reply at 1-2

Kesanupalli's Concern Is Bad Password Practices

Although passwords are commonly used to authenticate users, passwords are subject to various attacks. Such as phishing attacks, social engineering attacks, dictionary attacks and the like. Typically, longer passwords with combinations of letters and numbers provide a higher level of security. However, these longer passwords are more difficult for users to remember.

Issue: passwords are subject to various attacks that exploit bad passwords & users don't want to use complex passwords

Therefore, it is desirable to provide a user authentication method and system that provides a more secure authentication of the user than commonly used password-based methods and systems.

Solution: use biometrics and credentials that are bound to a website

IPR2024-00332, 512 PO Response at 6-7
IPR2024-00332, 512 PO Sur-Reply at 8-9
IPR2024-00334, 138 PO Response at 15-18
IPR2024-00334, 138 PO Sur-Reply at 4-5
Ex. 1006 (Kesanupalli) at 1: 1:36-41; 59-62

Dr. Goodrich: Kesanupalli Is Directed To A Secure Authentication System So That User's Use More Complex Password Practices

33. Kesanupalli states that passwords are typically used to authenticate user identity in authentication systems and procedures. Ex. 1006 at 1:27-28. Kesanupalli discusses issues with passwords. Ex. 1006 at 1:35-37. For example, phishing attacks and social engineering attacks can be used to compromise passwords. Ex. 1006 at 1:35-38. Phishing attacks compromise a user's credentials by sending a communication such as a text, email, call, or illegitimate website that tricks a user into disclosing his or her sensitive personal information. Social engineering attacks rely on manipulating a user to either share their sensitive personal information or trick users into compromising their account by taking insecure actions. As Kesanupalli explains, longer passwords with both letters and numbers are more secure, but Kesanupalli also recognizes that users may abstain from using longer and more complicated passwords because these passwords are more difficult to remember. Ex. 1006 at 1: 1:36-41. Kesanupalli states the desirability to have "a more secure authentication of the user than commonly used password-based methods and systems." Ex. 1006 at 1:59-62.

IPR2024-00332, Ex. 2037 (Goodrich 512 Decl.) at ¶ 33

IPR2024-00334, Ex. 2037 (Goodrich 138 Decl.) at ¶ 33

Demonstrative Exhibit - Not Evidence

Kesanupalli's Concerns Are Not Addressed By TPMs

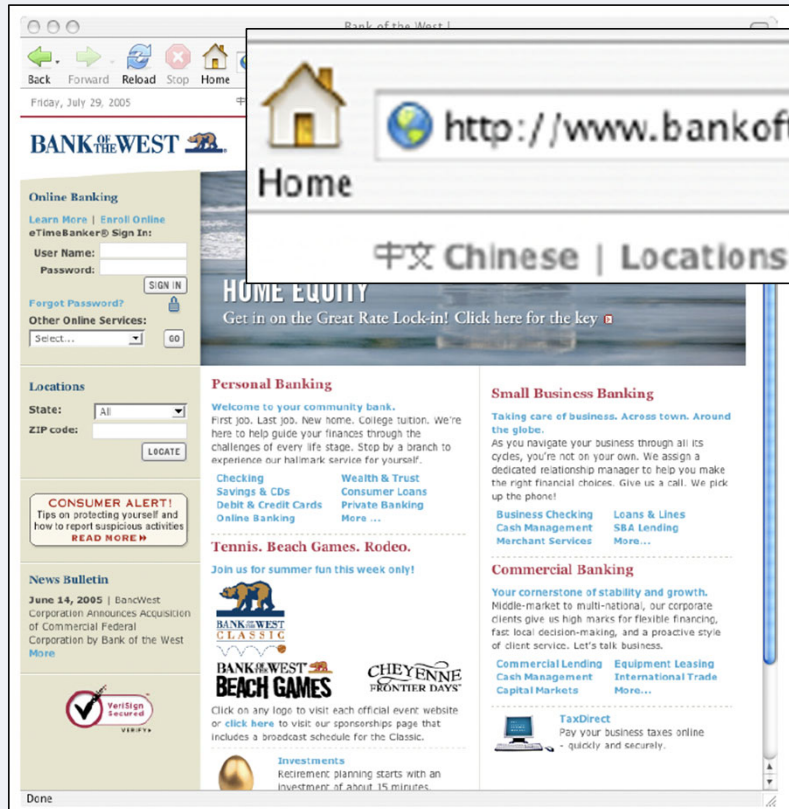
Although passwords are commonly used to authenticate users, passwords are subject to various attacks. Such as phishing attacks, social engineering attacks, dictionary attacks and the like. Typically, longer passwords with combinations of letters and numbers provide a higher level of security. However, these longer passwords are more difficult for users to remember.

A TPM has no impact on getting users to use better password practices so that they are not subject to the typical password attacks.

Therefore, it is desirable to provide a user authentication method and system that provides a more secure authentication of the user than commonly used password-based methods and systems.

IPR2024-00332, 512 PO Response at 6-7
IPR2024-00332, 512 PO Sur-Reply at 8-9
IPR2024-00334, 138 PO Response at 15-18
IPR2024-00334, 138 PO Sur-Reply at 2-3
Ex. 1006 (Kesanupalli) at 1: 1:36-41; 59-62

Dr. Goodrich: The Attacks Discussed In Kesanupalli Are Not Addressed By Adding A TPM



IPR2024-00332, Ex. 2037 (Goodrich 512 Decl.) at ¶ 47
IPR2024-00334, Ex. 2037 (Goodrich 138 Decl.) at ¶ 51

Dr. Goodrich: Kesanupalli is Concerned With Social Engineering Attacks And Attacks On Bad Password Practices.

56. Therefore, the Kesanupalli reference aims to reduce phishing risks by leveraging stronger passwords. In the Kesanupalli reference, **instead of requiring users to remember more complicated passwords, credentials are released only after checking biometrics that are bound to the web site (which, of course, would not match the web site address URL for a phishing web site)**. This enables a user to swipe a finger, which autofills credentials for a legitimate web site. This means that users do not need to remember complex credential information, like long, complex passwords, which reduces instances where users use or reuse basic passwords that are easier to recall, nor do users need to worry about checking whether a phishing web site address is close but different than a legitimate web site address. This occurs because users can choose passwords that are harder to remember without having to remember the passwords due to the fingerprint scan autofilling the password and the fingerprint (or other biometric) being bound to the particular legitimate web site address. This results in beneficial effects because basic passwords are vulnerable to phishing attacks compared to more complex passwords, e.g., due to users reusing a simple password at multiple web sites or using passwords that are in password dictionaries.

IPR2024-00332, Ex. 2037 (Goodrich 512 Decl.) at ¶ 52

IPR2024-00334, Ex. 2037 (Goodrich 138 Decl.) at ¶ 56

Dr. Goodrich: Adding A TPM To Kesanupalli Would Be Like Gold-Plating A Toothpick.

A POSITA – such as Ramesh Kesanupalli himself – would clearly understand this and that such a combination would be adding a superfluous component to a system that already is fully functional for its purpose, like adding gold plating to a toothpick. There is and was no reason or motivation for a POSITA to combine a TPM, such as that of the Challenger reference, with the Kesanupalli system.

IPR2024-00332, Ex. 2037 (Goodrich 512 Decl.) at ¶ 60

IPR2024-00334, Ex. 2037 (Goodrich 138 Decl.) at ¶ 64

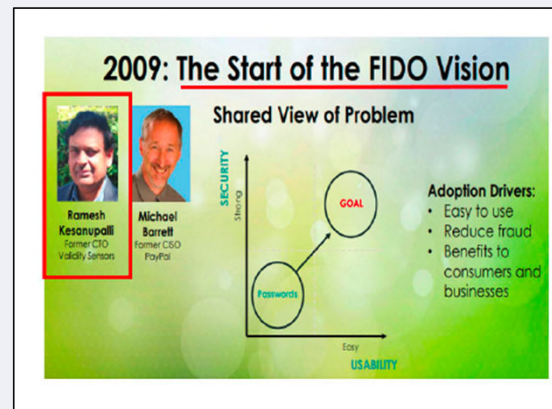
IPR2024-00332, 512 PO Response at 20

IPR2024-00335, 138 PO Response at 21

A POSITA—like Ramesh Kesanupalli—Would Have Been Well Aware Of TPMs.

Q. So secure elements were known before the introduction of mobile phones, right?

A. Oh, yeah, yeah, yeah. Yeah, I mean TPMS—in fact, one of the other FIDO founders, a guy called Ramesh [Kesanupalli], was part of the Trusted Computing Group which developed the original TPM standard.



Ramesh Kesanupalli

CEO of Digital Trust Networks and Co-Founder of the DID Alliance

As the Founder of Nok Nok Labs, Ramesh Kesanupalli brings to the company more than two decades of public and private sector IT security experience. Mr. Kesanupalli is responsible for representing the company as a board member of the FIDO Alliance, where he provides leadership to an industry consortium where Nok Nok Labs is a founding member. Mr. Kesanupalli previously served as the Chief Technology



IPR2024-00332, 512 PO Response at 9-10; Ex. 2040 (Redacted Transcript of Michael Barrett) at 91-92 (emphasis added); Ex. 2037 (Goodrich Decl.) at ¶37; Ex. 2039 (top); Ex. 2048 (bottom).

IPR2024-00335, 138 PO Response at 21

138 Patent Is Patenable Over The Art

Petitioner Has Failed To Show A POSITA Would Have Been Motivated To Combine Kesanupalli and Brown

Summary

The 512 Patent

1. The Art Does Not Render Obvious the Claims:

- Kesanupalli in light of Challenger does not teach or render obvious a second processor configured to “perform a secure backup of the record to a storage service or cloud storage.”

2. Apple’s Improper Broadening of Claims:

- Apple improperly relies on unclaimed embodiments to broaden the term *perform*.

3. Late Claim Construction Arguments:

- Apple did not seek to broadly construe *perform* and has waived its argument.

The 512 and 138 Patents

1. A POSITA Would Not Have Combined Kesanupalli with Challenger:

- A POSITA would not have added Challenger’s TPM to Kesanupalli’s system.

The 138 Patent

1. A POSITA Would Not Have Combined Kesanupalli with Brown:

- A POSITA would not have added Brown’s wiping capabilities to Kesanupalli’s system.

A POSITA Would Not Have Combined Or Modified Kesanupalli In Light Of Brown's Wiping Teachings

Apple Position

- A POSITA would have been motivated to combine Kesanupalli and Brown because “security threats [that] are multiple and multifaceted.”

Carbyne Response

- Wiping was known well before the priority date of Kesanupalli.
- Kesanupalli is interested in helping user's use better password practices.
- Kesanupalli has no need for a wiping feature.

IPR2024-00334, Pet. At 17-20
IPR2024-00334, PO Response at 18-21
IPR2024-00334, PO Sur-Reply at 4-5
IPR2024-00334, Pet. Reply at 12-14

Dr. Goodrich: A POSITA Would Not Have Considered Wiping Kesanupalli's System

69. Petitioner adds Brown for its wiping capabilities. Petition at 15, 19. Like adding a TPM, wiping a device would have no impact on deterring a social engineering attack. Once the attacker has tricked a user to release their credentials, wiping the device will not bring those credentials back or benefit the user in anyway. A POSITA would thus not have added Brown for the same reasons as discussed above with Kesanupalli and Challenger. Simply because a POSITA could add a wipe to Kesanupalli's system does not mean it makes sense to do so.

IPR2024-00334, Ex. 2037 (Goodrich 138 Decl.) ¶ 69

Summary

Summary

The 512 Patent

1. The Art Does Not Render Obvious the Claims:

- Kesanupalli in light of Challenger and Cheng does not teach or render obvious a second processor configured to *perform* a secure backup of the record to a storage service or cloud storage.

2. Apple's Improper Broadening of Claims:

- Apple improperly relies on unclaimed embodiments to broaden the term *perform*.

3. Late Claim Construction Arguments:

- Apple did not seek to broadly construe *perform* and has waived its argument.

The 512 and 138 Patents

1. A POSITA Would Not Have Combined Kesanupalli with Challenger:

- A POSITA would not have added Challenger's TPM to Kesanupalli's system.

The 138 Patent

1. A POSITA Would Not Have Combined Kesanupalli with Brown:

- A POSITA would not have added Brown's wiping capabilities to Kesanupalli's system.



ORAL ARGUMENT FOR IPR2024-00332 (10,929,512) & IPR2024-00334 (11,514,138)

Before Administrative Patent Judges

- Jameson Lee
- Arthur Peslak
- Steven Amundson