UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

_____

Case: IPR2024-00332
U.S. Patent No. 10,929,512

_____

DECLARATION OF DR. MICHAEL T. GOODRICH IN SUPPORT OF PATENT OWNER'S RESPONSE FOR U.S. PATENT NO. 10,929,512

TABLE OF CONTENTS

I. INTRODUCTION 1
II. BACKGROUND AND QUALIFICATIONS 1
III. MATERIALS REVIEWED 7
IV. LEGAL STANDARDS 8
V. PERSON OF SKILL IN THE ART 11
VI. CLAIM CONSTRUCTION 13
VII. BACKGROUND 13
A. '512 Patent 13
B. Asserted Art 15
1. Kesanupalli ("Secure User Authentication Using Biometric Information"; Ex. 1006) 15
2. Challener ("Apparatus and Method for Enabling Applications on a Security Processor"; Ex. 1007) 17
3. Ramesh Kesanupalli and David Challener 19
4. Cheng (System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information; Ex. 1008) 20
C. Trusted Platform Modules 21
VIII. THE '512 PATENT IS NOT INVALID BASED ON THE ASSERTED ART 23
A. A POSITA would not combine Kesanupalli and Challener 23
1. Ramesh Kesanupalli deliberately chose not to use a TPM 24
2. TPMs had many drawbacks 36
B. Cheng combined with Kesanupalli and Challener 37
1. The combination of Cheng with Challener and Kesanupalli does not disclose a second processor configured to perform a secure backup of the record to a storage service 37
2. A POSITA would not have reasonably expected Cheng to work with the Kesanupalli and Challener combination 41

3. Dependent Claims 2 and 12 43
4. Independent Claims 11 and 21 and Dependent Claims 44
IX. CONCLUSION 44

I, Michael T. Goodrich declare as follows:

I. INTRODUCTION

1. I have been retained by Patent Owner Carbyne Biometrics, LLC ("Carbyne") as an independent expert consultant in this proceeding before the United States Patent and Trademark Office ("PTO") against Apple Inc. ("Petitioner") regarding U.S. patent No. 10,929,512 ("the '512 Patent"). I have been asked to consider whether certain references disclose or suggest the features recited in claims 1–6, 10–16 and 20–21 ("the Challenged Claims") of the '512 Patent. My opinions are set forth below.

2. I am being compensated at my customary rate of $800 per hour for my work in this proceeding plus reimbursement of direct expenses. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

II. BACKGROUND AND QUALIFICATIONS

3. My educational background, career history, publications, and other relevant qualifications provided here are only a summary.

4. Based on my education, research, and work experience, I am knowledgeable about the subject matter of the '512 Patent and the related prior art.

5. I have over 35 years of experience in computer science, including the

topics of databases (including searching and indexing). For instance, in my peer-reviewed paper, C-103, which, according to Google Scholar, has been cited over 100 times, my coauthors and I introduce novel techniques for organizing the indexing structures of how data is stored so that alterations from an original version can be detected, and the changed values specifically identified. Further, my patent, U.S. Patent No. 7,299,219, "High Refresh-Rate Retrieval of Freshly Published Content using Distributed Crawling," which according to Google Scholar has been cited over 100 times, is directed at search engines, claiming a system for gathering fresh information added to a network such as the Internet and for processing the gathered fresh information (such as financial news), where a link server sends a batch of links to check to a crawler, which then executes its crawling assignment by filtering the encountered content and extracting only that which is new or changed. Also, my patent, U.S. Patent No. 9,152,716, is directed to an improved search engine technique that allows a user to ensure that an untrusted search engine provides complete and correct search results without requiring large proofs for large data collections, using techniques for a trusted crawler to index a distributed collection of documents and create an authenticated search structure that allows an untrusted search server to return reliably complete and correct search results. In my capacity as a Distinguished Professor at University of California, Irvine, my responsibilities include teaching undergraduate and graduate students, performing research in

computer science, mentoring PhD students and postdoctoral fellows, and serving on various university committees. I have held this distinguished position since July 2019 and I have been a professor at the University of California, Irvine since 2001. I have also served as an associate dean in the School of Information and Computer Sciences and as department chair for the Department of Computer Science.

6. Prior to my current position, I was a member of the faculty in the Department of Computer Science at Johns Hopkins University from 1987 to 2001, where my responsibilities included teaching, performing research in Computer Science, and serving on university committees.

7. I obtained a PhD in Computer Sciences from Purdue University in 1987. I also obtained a B.A. in Mathematics and Computer Science from Calvin College, which is now known as Calvin University, in 1983.

8. I have taught undergraduate and graduate courses concerning algorithms, data structures, software design, networking, and computer security beginning with my work as a graduate student at Purdue in 1983 and continuing as a professor at Johns Hopkins and University of California, Irvine. In addition, I have taught courses on algorithms and Internet technologies, including how web browsers and search engines work, at Johns Hopkins, UC-Irvine, and during a sabbatical at Brown University. I supervise a research team that has, over the years, comprised over twenty PhD students and several postdoctoral fellows. My current focus of our

research concerns networking, computer security, algorithm design, parallel and distributed computing, and data structures.

9. As shown in my CV, I have authored or coauthored over 350 peer-reviewed publications, and I have served as an editor and peer reviewer for scholarly publications and journals, including refereed conference proceedings on the topics of networking, computer security, parallel computing, databases, and algorithms. I have also published several books concerning algorithms, data structures, and computer security, including Algorithm Design and Applications, published by Wiley, and Introduction to Computer Security, published by Addison-Wesley. Further, I have published research papers on topics dealing specifically with financial data, financial documents, and financial transactions. For example, in my paper, C-101, which was published and presented at the International Conference on Financial Cryptography and Data Security, my coauthors and I presented computationally "lightweight" schemes for performing biometric authentication that carry out the comparison stage without revealing any information that can later be used to impersonate the user (or reveal personal biometric information). Unlike some previous computationally expensive schemes, which make use of slower cryptographic primitives, this paper presents methods that are particularly suited to financial institutions that authenticate users with biometric smartcards, sensors, and other computationally limited devices. Also, in my papers, C-83, C-85, and C-87,

my coauthors and I developed techniques to allow for untrusted content distributors, such as financial news and stock quote aggregators, to be able to publish financial data and documents so that users who query the information are presented with both the information and a cryptographic proof of its authenticity. In addition, in my papers, C-84 and C-151, my coauthors and I presented protocols for improving the security, privacy, and profitability of online auctions. Further, publications P-3. P-6, P-8, J-63, J-71, J-78, C-83, C-85, C-91, C-92, C-101, C-113, C-119, C-126, O-9, and O-13 specifically address authentication.

10. I am a Fellow of several industry and professional organizations, including Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), and American Association for the Advancement of Science (AAAS). I also regularly attend and present at computer science conferences concerning algorithms, networking, and computer security, including SIAM Symposium on Discrete Algorithms (SODA), ACM Symposium on Computer and Communications Security (CCS), and ACM Symposium on Parallelism in Algorithms and Architectures (SPAA).

11. I have received several awards and recognitions for my work concerning algorithms and distributed computing, including the Dean's Award for Research in the School of Information and Computer Sciences at University of California, Irvine ("for contributions in the area of parallel and distributed

algorithms"), the Robert B. Pond Sr. Award for Excellence in Undergraduate Teaching from Johns Hopkins University, the IEEE Computer Society Technical Achievement Award ("for outstanding contributions to the design of parallel and distributed algorithms for fundamental combinatorial and geometric problems"), and the Chancellor's Award for Excellence in Fostering Undergraduate Research from Univ. of California, Irvine. In addition, I have been elected as a foreign member of the Royal Danish Academy of Sciences and Letters.

12. I am an inventor on four U.S. patents, including US 7,257,711, "Efficient Authenticated Dictionaries with Skip Lists and Commutative Hashing," which discloses methods for authenticating information that is distributed from centralized servers through third-party information distributors, US 7,299,219, "High Refresh-Rate Retrieval of Freshly Published Content using Distributed Crawling," which, as I mentioned above, discloses a system for retrieving highly refreshed information quickly from Internet sources, US 8,681,145, "Attribute Transfer Between Computer Models Including Identifying Isomorphic Regions in Polygonal Meshes," which discloses technology for finding matchings between different geometric models, and US 9,152,716, "Techniques for Verifying Search Results Over a Distributed Collection," which, as I mention above, discloses a technology for verifying information that is extracted by web crawling processes on the Internet.

13. A copy of my curriculum vitae listing my full employment history is included as Exhibit 2038.

III. MATERIALS REVIEWED

14. The opinions contained in this declaration are based on the documents I reviewed, my professional judgment, as well as my education, experience, and knowledge regarding security, device architecture, communications, and coding.

15. In forming my opinions expressed in this declaration, I reviewed the following materials and information:

Number	Title
1001	U.S. Patent No. 10,929,512 to Jakobsson et al. ("the '512 Patent")
1002	File History of U.S. Patent No. 10,929,512
1006	U.S. Patent No. 8,799,666 ("Kesanupalli")
1007	U.S. Patent No. 8,099,789 ("Challener")
1008	U.S. Patent Publication No. 2004/0117636 ("Cheng")

Number	Title
2038	CV of Dr. Michael Goodrich
2039	FIDO Presentation of Ramesh Kesanupalli
2040	PUBLIC Excerpts of the deposition transcript of Mr. Micheal Barrett
2041	David Challener & Will Arthur, A Practical Guide to TPM 2.0 (Apress 2015)
2042	David C. Challener & J. D. Osborn, Trusted Platform Module Evolution (2015)
2043	Rachna Dhamija, J.D. Tygar & Marti Hearst, Why Phishing Works, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06) 581 (2006), https://doi.org/10.1145/1124772.1124861.
2044	S Sinclair, SW Smith, The TIPPI point: Toward trustworthy interfaces, IEEE Security & Privacy 3 (4), 68-71, 2005

Number	Title
2045	Ramesh Kesanupalli, LinkedIn Profile, https://www.linkedin.com/in/ramesh-kesanupalli-22b73/ (accessed Oct. 5, 2024)
2046	Dave Challener, LinkedIn Profile, https://www.linkedin.com/in/dave-challener-bbab7b/ (accessed Oct. 5, 2024)
2047	Nok Nok, About, https://noknok.com/about/ (accessed Oct. 5, 2024)
2048	Ramesh Kesanupalli, Team, Nok Nok, https://noknok.com/about/team/ramesh-kesanupalli/ (accessed Oct. 5, 2024)
2049	Federal Trade Commission, How to Recognize and Avoid Phishing Scams, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (accessed Oct. 5, 2024)
2050	Microsoft, Introduction to Windows Biometric Framework, https://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/wbfintro.docx (accessed Oct. 5, 2024)
2051	ISO/IEC 11889-1:2009, Information Technology — Trusted Platform Module — Part 1: Architecture (2009).

16. I also reviewed any other materials I refer to in this declaration in support of my opinions.

17. My opinions contained in this declaration are based on the documents I reviewed and my knowledge and professional judgment. My opinions have also been guided by my understanding of how a person of ordinary skill in the art would have understood the state of the art, the prior art, and the claims and the specification of the ’512 Patent at the time of the alleged invention.

IV. LEGAL STANDARDS

18. As a technical expert, I am not offering any legal opinions. Rather I am offering technical assessments and opinions. In rendering my analysis, I have been

informed by counsel regarding various legal standards for determining patentability. I have applied those standards in forming my technical opinions expressed in this report.

19. The patent claims describe the invention made by the inventors and describe what the patent owner owns and what the owner may prevent others from using. I understand that an independent claim sets forth all the requirements that must be met to be covered by that claim. I further understand that a dependent claim does not itself recite all of the requirements of the claim but refers to another claim and incorporates all of the requirements of the claim to which it refers.

20. It is my understanding that a claimed invention is unpatentable if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Obviousness, as I understand it, is based on the scope and content of the prior art, the differences between the prior art and the claim, and the level of ordinary skill in the art. I understand that a claim could have been obvious from a single prior art reference or from a combination of two or more prior art references.

21. I understand that when evaluating obviousness, one must not consider whether the claimed invention would have been obvious to a layman or to an expert; not use hindsight when comparing the prior art to the claimed invention; not consider

what was learned from the teachings of the patent. In particular, I understand that it is improper to use the patent claims as a road map for selecting and combining items of prior art. In other words, one should avoid using the challenged patent as a guide through the prior art references, combining the right references in the right way so as to achieve the result of the claims at issue. Instead, one must put oneself in the place of a person of ordinary skill at the time the invention was made and consider only what was known before the invention was made and not consider what was only known after the invention was made.

22. I understand that obviousness should be considered in light of the problems known to the person having ordinary skill in the art at the relevant time and the complexity of the alternatives for solving the problem. That individual elements of the claimed invention are disclosed in the prior art is not alone sufficient to reach a conclusion of obviousness.

23. I understand that certain factors (also called secondary considerations) may support or rebut the obviousness of a claim. I understand that such secondary considerations include, for instance, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected results of the invention, any long-felt but unsolved need in the art that was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art,

and copying of the alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention. I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness.

24. I also understand that while it may be helpful to identify a reason for a combination, common sense should guide the analysis and no rigid requirement of finding a teaching, suggestion, or motivation to combine is required. When a product is available, design incentives and other market forces can prompt variations of the product, either in the same field or different one. If a person of ordinary skill in the art can implement a predictable variation, obviousness likely bars its patentability. For the same reason, if a technique has been used to improve one device and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique would have been obvious. I understand that a claim would have been obvious if common sense directs one to combine multiple prior art references or add missing features to reproduce the alleged invention recited in the claims.

V. PERSON OF SKILL IN THE ART

25. It is my understanding that Petitioner contends the following definition is the level of ordinary skill in the art:

> "Here, Persons of Ordinary Skill in the Art ("POSITA") at the time of the claimed invention would have had a bachelor's degree in an electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa. Furthermore, a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard for POSITA."

Petition at 6.

26. I apply the Petitioner's POSITA for the sake of my opinions herein. Now and as of the priority date of the '512 Patent, I met the level of skill described above. Further, I have taught thousands of undergraduate and graduate computer science students since 1987, including on topics relevant to the research, design, development, and/or testing of authentication techniques, and related firmware and software; hence, I have extensive experience with respect to the knowledge of a POSITA.

27. Thus, based on my knowledge and experience, I understand what a person of ordinary skill in the art would have known at the times of the alleged

invention. My opinions herein are, where appropriate, based on my understandings as to a person of ordinary skill in the art at those times.

VI. CLAIM CONSTRUCTION

28. It is my understanding that Petitioner contends a plain and ordinary meaning for the term "restricted interface." Petition at 7-8. My opinions herein do not depend on this definition. Accordingly, I do not address the meaning of that term.

VII. BACKGROUND

A. '512 Patent

29. The '512 Patent is titled "Authentication Translation," which was filed on January 27, 2020 and claims priority through a sequence of continuations and applications to as early as December 9, 2011. *See* Ex. 1001. Prior authentication technologies provided a "tedious" user experience when credentials were provided to a service, thereby causing users to re-use passwords and select weaker passwords. Ex. 1001 at 1:35-40. Consequently, users had less secure accounts and were more prone to be the victim of a social engineering attacks, like phishing. Ex. 1001 at 1:37-40. This led to a need for authentication technologies to improve as acknowledged by the patent itself. Ex. 1001 at 1:40-42. Addressing this need, the '512 Patent disclosed an innovative approach that did not require users to type their passwords, which increased the likelihood that users would chose complicated passwords and practice other stronger password practices:

> "[U]sers need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an 'authentication translator' via an appropriate technique, and the authentication translator will provide the appropriate credentials to the implicated service on the user's behalf."

Ex. 1001 at 2:62-3:1.

30. As illustrated in reproduced Figure 3 below, the '512 Patent's novel approach utilizes a unique hardware architecture can protect user credentials, by segregating processing capabilities between two processors 304/308 and the insecure memory 302 from secure storage 306:

> "[A] mobile phone 300 includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (e.g., a camera or a fingerprint reader). Users (and applications) can read from and write to the insecure storage area. However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API."

Ex. 1001 at 3:66-4:8.

31. This segregation of processing and storage/memory in turn separates allows the system to keep the user's credentials safe from malware that may breach

the (application) processor 304.

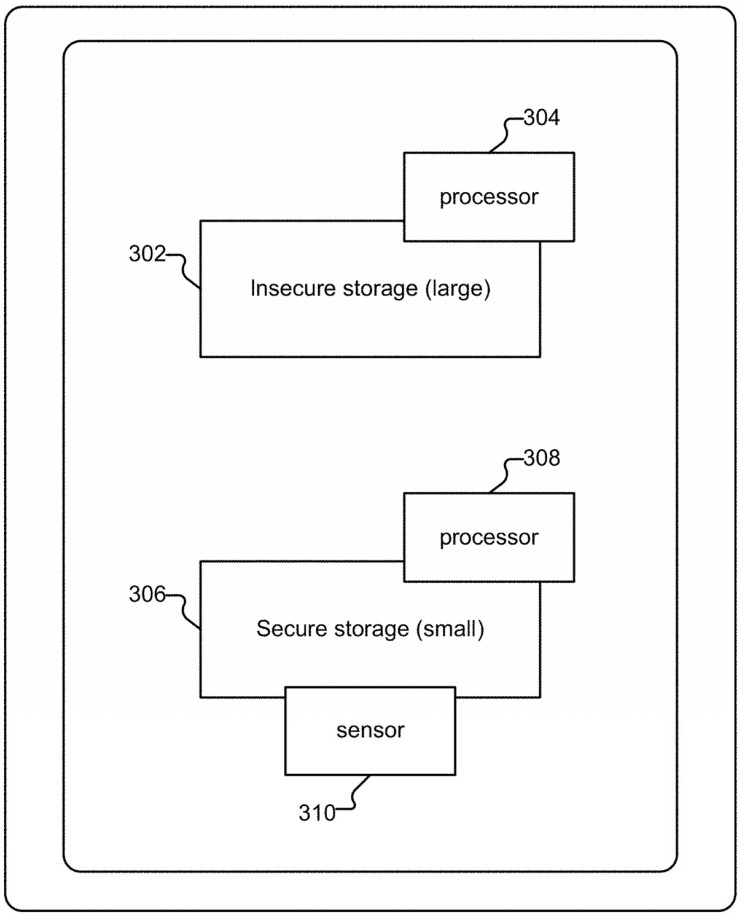


FIG. 3

B. Asserted Art

32. I now provide an overview of the prior art.

1. Kesanupalli ("Secure User Authentication Using Biometric Information"; Ex. 1006)

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.

34. Kesanupalli discloses a system that stores fingerprint templates and user credentials in a secure storage device and releasing credentials from the secure storage only after a fingerprint template matching a fingerprint scan, which allows users to use more complicated passwords without needing to remember the passwords. Ex. 1006 at 3:14-4:11. For example, Kesanupalli describes the architecture illustrated in Figure 2 below in its specification. The sensor decrypts

user credentials after confirming a match and uses the SSL protocol to communicate with the Host PC. Ex. 1006 at 6:31-49. The biometric service executes on the Host PC. Ex. 1006 at 5:62-64. The biometric service can communicate with applications, such as web servers connected through the internet, that request user authentication. Ex. 1006 at 5:62-64, 6:11-25. For instance, Kesanupalli discloses that example applications include Internet browser applications, financial applications, and the like, and that its system can utilize an application programmer interface (API) such as a Windows API (e.g., WinUSB Driver) for secure communications between the PC and the biometric sensor. Ex. 1006 at 5:65-6:10.

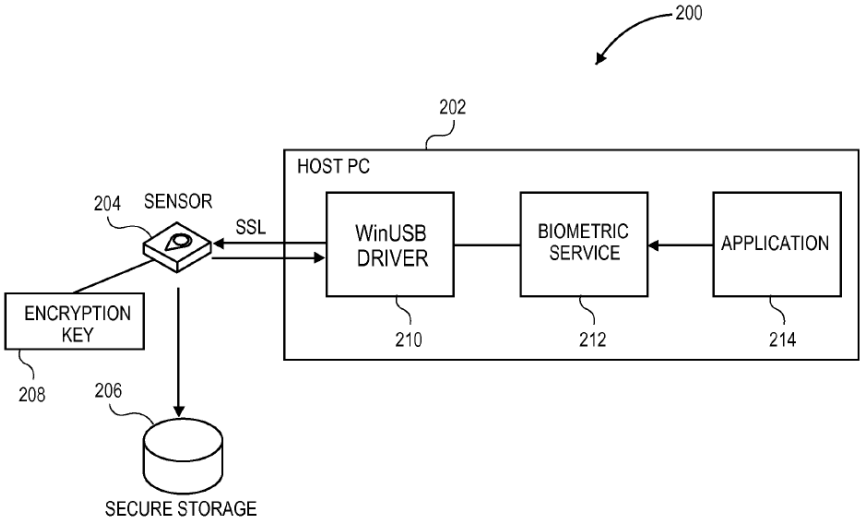


FIG. 2

Ex. 1006 at Figure 2.

2. Challener ("Apparatus and Method for Enabling Applications on a Security Processor"; Ex. 1007)

35. Challener "relates to securely protecting computer data, and more

particularly to security processors provided in computer systems to implement security features." Ex. 1007 at 1:7–9. Challener discloses a system with an input portion that allows user to input data into the system, such as through a smartcard reader, keyboard, or fingerprint reader. Ex. 1007 at 3:58-4:1. These input devices can be used to authenticate a user. Ex. 1007 at 4:1-3. A security portion includes a processor and nonvolatile memory that "secure the data and applications of the system for access and use only by authorized users." Ex. 1007 at 4:9-11. Challener's system can use the Trusted Computing Group's Trusted Platform Module (TPM or TPMs plural). Ex. 1007 at 1:18-20, 3:46–62, 4:24–43. The processor "is dedicated to security functions" and can be a Trusted Platform Module (TPM or TPMs plural). Ex. 1007 at 4:11-14, 4:24-43. A standard portion includes a CPU, memory, a storage device, and output devices. Ex. 1007 at 4:15-21.

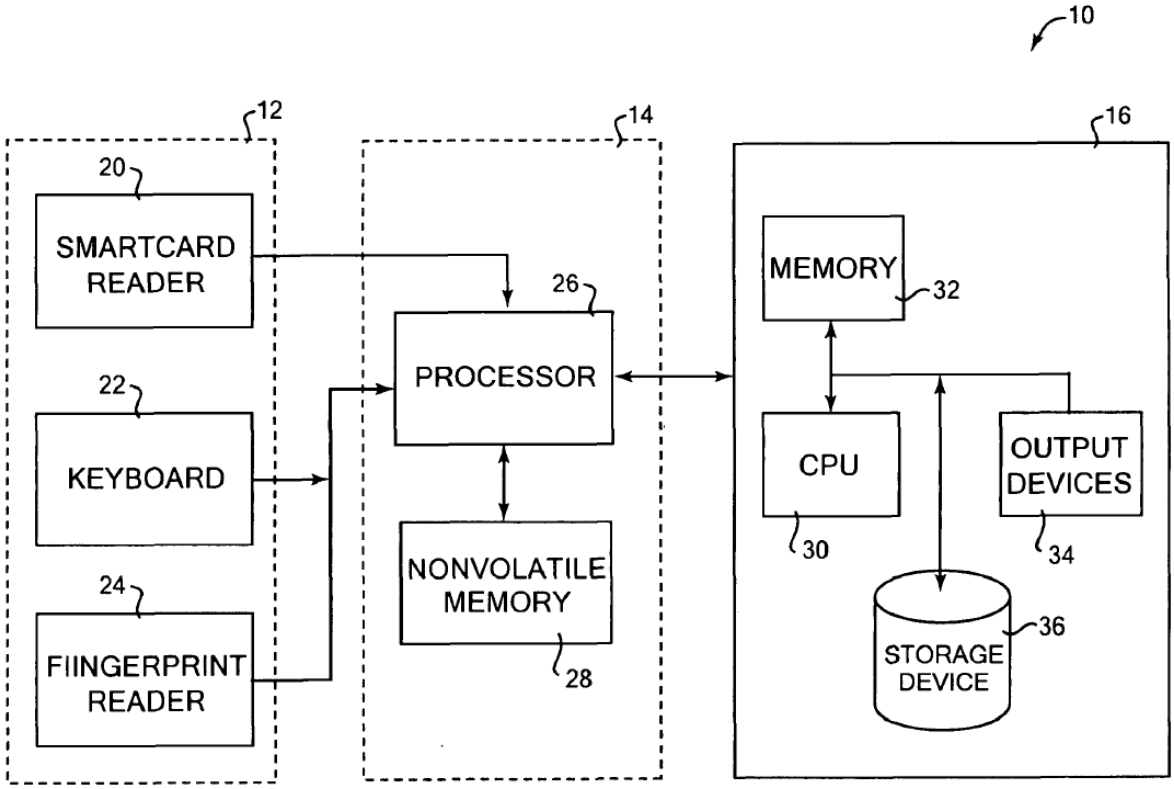


FIG. 1

Ex. 1007 at Figure 1.

3. Ramesh Kesanupalli and David Challener

36. The authors of the Kesanupalli and Challener references were leading innovators in secure computing and secure authentication. This is clearly illustrated by Ramesh Kesanupalli's and David Challener's professional experiences, for example, not to mention their co-inventors.

37. Ramesh Kesanupalli is a pioneer in the field of identity management and authentication. Ex. 2044 at 69-71; Ex. 2045. He founded Nok Nok Labs. Nok Nok Labs provides next-generation authentication solutions, as evident from its

about page: "Nok Nok is a leader in passwordless customer authentication and delivers the most innovative FIDO, (Fast IDentity Online), solutions for the passwordless authentication market today." Ex. 2047. Nok Nok's association with FIDO extends to Ramesh Kesanupalli. Ex. 2048. He was a founder of the FIDO (Fast Identity Online) Alliance, which identifies the start of its vision as beginning in 2009 with the work of Ramesh Kesanupalli and which focuses on open authentication standards. Ex. 2039. Ramesh Kesanupalli "was part of the Trusted Computing Group, which developed the original TPM standard." Ex. 2040. Accordingly, Ramesh Kesanupalli was intimately aware of TPMs.

38. David Challener is also a pioneer in trusted computing and was "active in the TCG, serving on the Board of Directors, chairing the TSS Workgroup, and participating in the Technical Committee, Virtualization Workgroup, and Storage Workgroup." Ex. 2042 at 543. Further, David Challener "currently cochairs the TPM Working Group." *Id.*; Ex. 2046. Similarly, David Challener was intimately aware of TPMs.

4. Cheng (System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information; Ex. 1008)

39. Cheng discloses a method to "backup and restore a user's portable biometrics-based authentication device without compromising the secrecy." Ex. 1008 at [Abstract]. Cheng uses a two-tier encryption structure. Ex. 1008 at

[Abstract], [0007]-[0009]. Upper tier data contains user biometric information along with encrypted lower tier data. Ex. 1008 at [Abstract]. Lower tier data contains authentication information and electronic identity information in an encrypted form. Ex. 1008 at [Abstract]. Lower tier data can only be decrypted after decryption and validation of upper tier data. Ex. 1008 at [Abstract], [0007]-[0009].

C. Trusted Platform Modules (TPM or TPMs)

40. A TPM is a "standards-based embedded security subsystem on the motherboard." Ex. 2042 at 539. Both TPM 1.0 and 1.2 were introduced in the early 2000s, but TPMs were not substantially used in the 2000s, with hampered adoption being acknowledged by David Challener:

> "[A]lthough the TPM 1.1b and 1.2 specifications created the foundation for the use cases described, a number of roadblocks occurred that hampered adoption by industry. These included ambiguities in the specification, rigidness in the policy regarding how keys are used, tight coupling to specific cryptographic algorithms, and issues related to control of the TPM by platform software."

Ex. 2042 at 1-3.

41. Hardware adoption was only one bottleneck to TPM adoption. As time

passed, TPM utilization lagged behind hardware inclusion because applications did not require them. Consistent with TPM adoption continuing to lag years after the priority date of the '512 Patent, David Challener wrote that in 2015 TPMs were "nearly ubiquitous" but TPMs were nonetheless "mostly invisible to uses due to a lack of compelling applications to use them." Ex. 2041 at 1. As a result of these prevalent adoption issues, operating system providers refrained from requiring TPMs until approximately a decade after the TPM 1.0 specification was initially published. *Id*. at 536. For example, Windows did not require TPMs until January of 2015. *Id*.

42. Software use of TPMs lagged even further behind hardware inclusion of TPMs in devices. While TPMs were sometimes included by device manufacturers in their devices, TPMs were commonly not enabled by default. *Id*. at 536 ("Microsoft has announced that all systems submitting to the Windows Certification Program after 1 January 2015 will be required to have TPM 2.0."); *Id*. at 542 ("Without question, the biggest hindrance to widespread adoption of TPM 1.2 is that PC vendors ship machines with the TPM turned off by default.").

43. In summary, TPMs were not being enabled by default and were not being required by operating system providers. As a result, TPMs were not used in most devices, regardless of whether the device may or may not have had a TPM. Id. at 539 ("Because most users never touch their firmware settings, this means that

most TPMs have never been turned on."). This meant that most TPMs at the time of invention were mere ornamentation rather than functional to a device. Despite these widespread adoption issues, TPMs would have been known to a POSITA at the time of the invention. For example, TPM 1.2 was an ISO/IEC standard by 2009. Ex. 2051.

VIII. THE '512 PATENT IS NOT INVALID BASED ON THE ASSERTED ART

44. In my opinion, the '512 Patent is novel and non-obvious. First, Petitioner does not show that a POSITA would have combined Kesanupalli's fingerprint sensor with Challener's TPM. Second, Petitioner does not show the combination of Cheng's backup method with the combination of the Kesanupalli reference and the Challener reference discloses a second processor that *performs* a secure backup of a record *to* a storage service. Third, Petitioner does not show the dependent claims' unique elements are taught. This is discussed in greater detail below.

A. A POSITA would not combine Kesanupalli and Challener

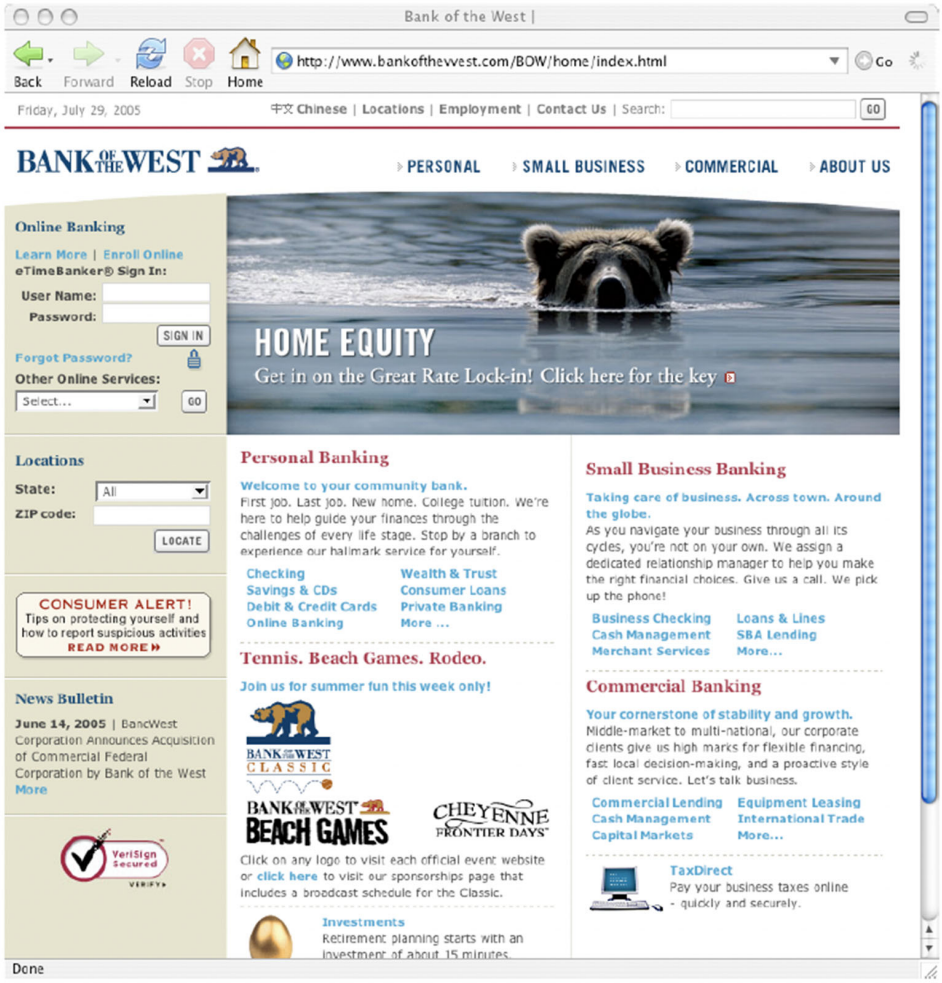
45. A POSITA would not have combined the Kesanupalli reference with the Challener reference. Ramesh Kesanupalli was a computing security leader and a Trusted Computing Group member that was himself a POSITA. As explained above, Ramesh Kesanupalli was aware of TPMs but nonetheless chose not to use TPMs in the Kesanupalli reference. Ramesh Kesanupalli's design choices illustrate what a

POSITA would have done and the reasons why a POSITA would have done so.

1. Ramesh Kesanupalli deliberately chose not to use a TPM

46. The Kesanupalli reference addresses social engineering attacks, which includes phishing. Ex. 1006 at 1:35-37. These attacks rely on tricking users to release credentials, which can occur by emailing or texting links to legitimate looking fake websites that a user enters personal information to thereby compromise their legitimate account.

47. An example of a phishing web site attack, trying to trick a user to type in their username and password credentials for a bank is shown below:



Ex. 2043 at 587.

48. This is an example of a phishing attack that uses a fake web site address that looks at first to be that of the Bank of the West, but upon closer inspection one can see that the web address makes use of two "v"'s instead of a "w" in a web address URL. A user who is not looking very carefully could miss this and enter their username and password credentials into the web page, which would then give those credentials to an attacker.

49. Another example of a phishing attack is a phishing email, such as that

shown below:

Ex. 2049.

50. As shown in the image above, a user receives an email. The email is from an illegitimate source — a sender other than Netflix in this example (i.e., in fact not "Your friends at Netflix" as the email falsely states), but it nevertheless appears to be from a legitimate source. The email threatens the user by claiming "Your account is on hold." The email then claims there is an issue with billing information that needs to be updated. This message invites a user to fix the claimed issue by clicking the big red rectangle with the text "UPDATE ACCOUNT NOW." This button contains a link to an illegitimate website that impersonates the legitimate Netflix website. When a user is tricked into clicking this button, the user enters sensitive information such as Netflix credentials and personal information (e.g.,

credit card information, address information, security question answers, etc.). The illegitimate source then has access to all this personal information. In many cases, the tricked user is unaware of the fact that they provided this sensitive information to an illegitimate source, which provides an illegitimate source with a longer window to exploit this sensitive information without detection.

51. After an attacker obtains sensitive information, the attacker can access compromised accounts to commit additional fraud. This additional fraud may be difficult for a victim to identify and track in many cases. These and other weak password practices (*e.g.*, shorter passwords without combinations of letters and numbers) are more susceptible to phishing attacks, which the Kesanupalli reference aims to discourage. Ex. 1006 at 1:37-39. The Kesanupalli reference's aims are not furthered by TPMs, which provide device security. A POSITA would recognize this fact, and would not have been motivated to add the TPM architecture of Challener to Kesanupalli as it does not address these attacks. For example, if a user was tricked into providing their credentials to a phishing web site, it provides no additional security for the user to have used a TPM and fingerprint reader to unlock those credentials before sending them to the fake web site.[1] Accordingly, Ramesh

[1] Kesanupalli avoids this risk without using a TPM, e.g., by using a Web browser plug-in and binding biometric data to the web site. Ex. 1006 at 4:36-5:58, 8:2-53.

Kesanupalli (a POSITA) would not have been motivated to add a TPM to the Kesanupalli reference, which is further evidenced by the fact that Ramesh Kesanupalli in fact did not include a TPM in the Kesanupalli reference.

52. 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.

53. As discussed above with regards to the phishing examples, phishing often attempts to redirect the user to an illegitimate website that mimics the legitimate site in order to obtain sensitive information from the user. The Kesanupalli reference binds credentials to websites in order to avoid autofilling credentials on an illegitimate website. This feature further reduces phishing risks because users cannot be deceived into providing credentials on an illegitimate website, which would not be bound to a user's biometric.

54. Adding a TPM to the Kesanupalli reference would not aid in reducing such social engineering attacks because these social engineering attacks trick a user into providing their credentials to illegitimate sources or use prevalent techniques to breach common passwords. If a user is tricked to unlock their credentials, even using biometric data and a TPM, they could then send that data to a phishing web site; hence, the TPM provides no additional security to the Kesanupalli reference. Instead, it is the **binding** of the biometric to the legitimate web site that provides the security in the invention of the Kesanupalli reference. An example of another common social engineering attack technique is a dictionary attack, which attempts to access an account through the use of a list of common passwords. A dictionary attack can compromise credentials that use a common password simply by guessing the password from the password list until the right password is guessed and access to an account is obtained. As with a phishing attack based on a fake web site that is not

bound to biometric data, a TPM would not aid in reducing dictionary social engineering attacks because the TPM is for device side security while social engineering attacks occur outside the device. For example, even if a user stored a simple password (that is included in a common password list) in the secure memory of a TPM, that provides no additional security, since an attacker can simply try all the passwords in the password list and discover the user's password without breaking the security of the TPM. Accordingly, a POSITA would understand that adding a TPM to the Kesanupalli reference would have no benefit for protecting against the social engineering attacks contemplated by the Kesanupalli reference.

55. Instead, a POSITA would understand the Kesanupalli reference to be teaching that secure systems need to **educate users** to protect themselves against phishing attacks along with providing a system that facilitates phishing-attack protection. For example, Kesanupalli explains that longer passwords provide more protection than short passwords or passwords that can be found in password dictionaries. Ex. 1006 at 1:38-39 ("Typically, longer passwords with combinations of letters and numbers provide a higher level of security.") A problem that Kesanupalli identifies is that longer passwords (which are more secure) are more difficult for users to remember. Ex. 1006 at 13:39-41 ("However, these longer passwords are more difficult for users to remember."). Accordingly, the Kesanupalli invention is directed towards a system that supports users employing stronger

passwords without having to memorize them and thereby provide increased security by combining these stronger passwords with a secure system using biometrics and bindings between web sites and these biometrics. Ex. 1006 at 1:59-62, 3:4-31.

56. Moreover, the Kesanupalli reference discloses a system that already provides an **end-to-end secure system**, which a POSITA would understand would not be made more secure with the addition of a TPM. For example, Kesanupalli discloses operating system drivers, biometric services, and applications, such as browsers, together with secure browser plug-ins. Ex. 1006 at Fig. 2, 2:54-67, 4:36-63. Further, Kesanupalli discloses that all such software binary files are digitally signed and authenticated prior to running the binary file, as well as being validated at runtime. Ex. 1006 at 8:23-28. For instance, Kesanupalli discloses that such techniques block malicious attempts to replace or edit the binary files. *Id.* Thus, a POSITA would understand that the Kesanupalli reference is not aimed at preventing credentials from being communicated to a browser or browser plug-in, since these binary files are constantly being checked for modifications, such as would occur from the injection of malware. For instance, Figure 11 of the Kesanupalli reference illustrates an enrollment process where user biometric information is provided to a browser extension, which is highlighted below. Ex. 1006 at Fig. 11, 2:2-21. Figure 11 has "provide biometrics" in the "User" column. An arrow from "provide biometrics" is pointed at the "Biometric Browser Extension" column.

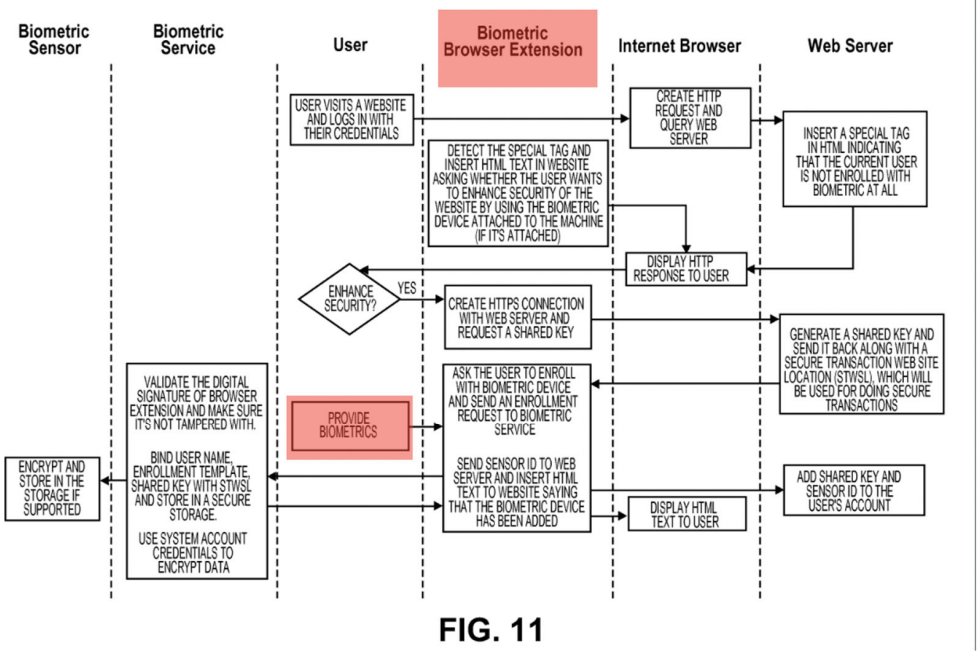


FIG. 11

Ex. 1006 at Fig. 11.

57. A POSITA would understand the Kesanupalli reference provides user biometric information to the biometric browser extension. Browser extensions run on the application processor, and this complete pipeline of software is digitally signed and validated at runtime. Ex. 1006 at 8:23-28. Consequently, the biometric information is accessible only by the pipeline of secure software (i.e., binary files) shown in Figure 2 (excerpted above), so malware cannot compromise credential information accessible to the application processor. Additionally, the Kesanupalli system protects the communication link between the biometric sensor and PC (which can utilize any type of communication, including USB) and between the PC and the web site. Ex. 1006 at Fig. 2, 2:50-53, 6:37-42, 7:28-32, 8:2-22. Accordingly, this

demonstrates plainly that the Kesanupalli reference was not directed to device protection against malware generally, since such attacks are already protected against in the Kesanupalli system. Instead, the Kesanupalli reference was directed squarely to protecting user credentials from illegitimate websites that trick users. Thus, for this additional reason, a POSITA would not be motivated to add a TPM to the Kesanupalli reference.

58. Figure 12 illustrates the Kesanupalli reference provides user biometric information to a browser extension and the biometric browser extension sends the web server the credential. Ex. 1006 at Fig. 12. As mentioned above, the Kesanupalli reference is aimed at social engineering and phishing attacks. Consequently, the Kesanupalli system securely provides credentials to the browser extension, which in turn securely provides credentials to a **legitimate** web site, e.g., as is also shown below.

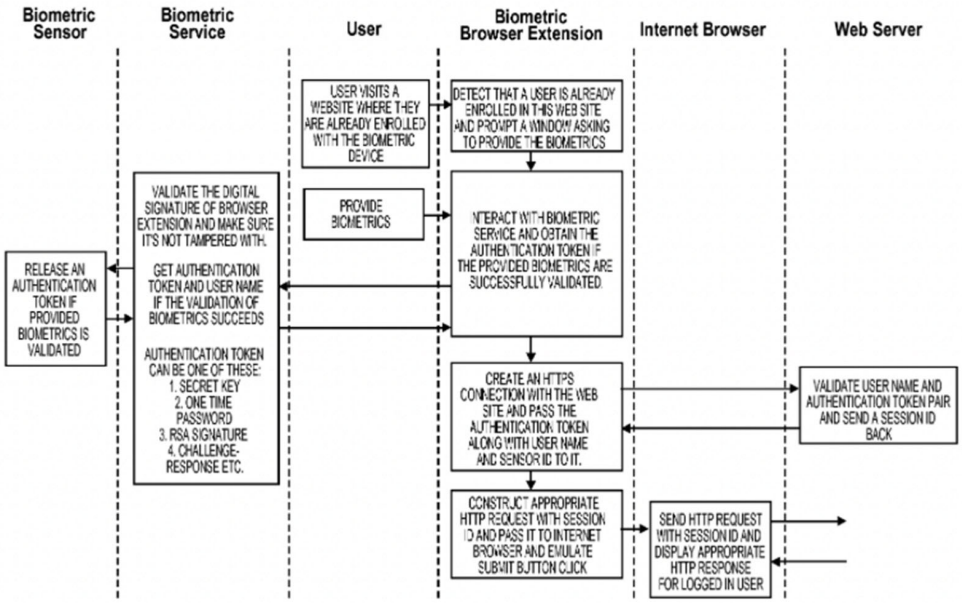


FIG. 12

Ex. 1006 at Fig. 12.

59. Kesanupalli's approach of providing sensitive information to the browser extension and website is in furtherance of preventing social engineering attacks rather than in furtherance of providing greater on-device security against malware. The Kesanupalli reference discloses that a cryptographic key is a credential that is transmitted directly "to a specific address, location, or other recipient identifier." Ex. 1006 at 3:41-44, 4:3-11. Therefore, user authentication occurs via a cryptographic key being sent to a web server. The Kesanupalli reference states that this transmission is protected. This stated protection is based on the cryptographic key being sent to a website that is confirmed legitimate rather than an illegitimate

imposter website attempting to gather user credentials. Ex. 1006 at 4:7-9. Thus, the Kesanupalli reference is aimed squarely at preventing social engineering attacks by providing sensitive biometric information and cryptographic keys to the biometric browser extension. This again plainly illustrates that the Kesanupalli reference was not directed to device protection against malware generally. For example, a POSITA would understand that malware that may have infected some other component of the PC could not corrupt the functioning of the credentials and biometric components of the Kesanupalli system, since, e.g., these components are digitally signed and checked for validity at runtime. Ex. 1006 at 8:23-28.

60. Because the Kesanupalli reference's system securely provides sensitive information to the application processor executing the biometric browser extension and to web servers receiving credentials, adding a TPM to the Kesanupalli reference's system would not result in security benefits. 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 Challener reference, with the Kesanupalli system. Based on these incompatibilities, I therefore conclude that a POSITA, including and especially Ramesh Kesanupalli himself, would not be motivated to include a TPM in the Kesanupalli system.

2. TPMs had many drawbacks

61. In addition to not providing additional security, a POSITA would understand that there would be drawbacks to adding a TPM to the invention of the Kesanupalli reference. For example, practical considerations regarding TPM adoption and deployment in 2012 would motivate a POSITA to consciously exclude the use of a TPM with the Kesanupalli reference.

62. TPM adoption was a slow process that stagnated due to many implementation and deployment challenges. In 2012, compatibility issues with existing systems and software could be caused by implementing TPMs. This is because mainstream systems and software did not support TPMs. These compatibility issues made TPM use less desirable to support because they either failed to work or were not used often. A lot of non-TPM security solutions were widespread and commercialized. Many non-TPM solutions offered compatibility with existing systems and software. Compatibility was a critical consideration for the Kesanupalli reference. Ex. 1006, at 3:64-4:3, 4:12-22, 5:44-6:10, 7:25-61.

63. In view of the need for compatibility, the Kesanupalli reference's preferred embodiment used the following: Windows Biometric Framework (WBF), WBF Interface, and the WinUSB driver. Ex. 1006 at 5:59-6:10, Figs. 1 and 2. Both operating systems and software did not generally require or support TPMs. Unsurprisingly, a TPM was not required by the WBF. Ex. 2050. Nor did Windows

require a TPM in 2012. Windows in 2012, as well as other major operating systems, did not require TPM use for all functionalities. TPMs were supported in Windows 7 and Windows 8. However, many features that used TPMs made TPMs optional as opposed to required. In fact, TPMs were disabled as a default setting in Windows. This highlights that adoption issues continued beyond the inclusion of TPM hardware in devices. If a user were to enable the TPM, the user would have to go through and complete multiple configuration steps and options that complicated and hampered user experiences. Furthermore, enabling and using TPMs had the potential consequence of creating compatibility issues. All of these support problems heavily discouraged TPM use at the time.

64. As TPMs were not required or implemented universally in 2012, TPMs would significantly narrow the applicability of systems such as the Kesanupalli reference to devices with enabled TPMs. Accordingly, there are many reasons from 2012 why Ramesh Kesanupalli would consciously choose not to use TPMs in his patented system and why a POSITA would not combine the Kesanupalli reference with a TPM, such as the TPM of Challener.

B. Cheng combined with Kesanupalli and Challener

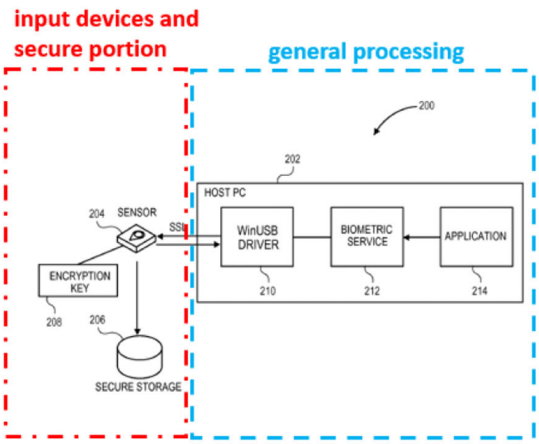
1. The combination of Cheng with Challener and Kesanupalli does not disclose a second processor configured to perform a secure backup of the record to a storage service

65. Petitioner has not shown the combination of the Kesanupalli reference

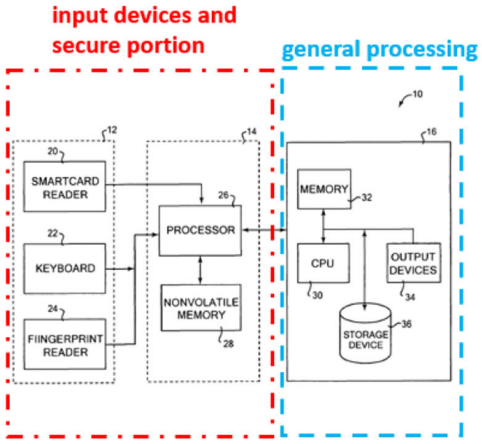
and the Challener reference combined with the Cheng reference discloses a "second processor configured to… perform a secure backup of the record to a storage service." Nor did Petitioner show a POSITA would have had a reasonable expectation of success in combining the combination of the Kesanupalli reference and the Challener reference combined with the Cheng reference. The Petitioner argues that modifying a TPM to include the backup method of the Cheng reference was "straightforward" because of the "widely practiced porting of code to a TPM environment." APPL-1019, APPL-1017, Petition at 55. Petitioner has not shown any reference disclosing a TPM backing up its records to any storage service. Nor has Petitioner shown any reference (including any reference from David Challener, who was an expert in the field of TPMs) where a TPM backed up its records to any storage service. This is unsurprising because this asserted combination would be very difficult to implement while protecting TPM data.

66. Petitioner in broad strokes combines the Challener reference's secure portion into the Kesanupalli reference's sensor, as illustrated below. Petitioner believes a POSITA would combine the Kesanupalli reference with the Challener reference because the TPM is isolated so its contents are secure. 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. Accordingly, the incorrect processor would perform any alleged backup.



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated

Petition at 20.

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. Accordingly, the TPM and sensor combination is not a processor that performs a secure backup *to* a storage service.

68. Petitioner's apparent position may be that the second processor need not *perform* a secure backup of the record *to* a storage service. The claim language clearly requires otherwise:

- Limitation 1.6B: "*facilitate* a login of the user to the external resource…"
- Limitation 1.7A: "*perform* a secure backup of the record to a storage service"

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. Accordingly, the combination of Kesanupalli, Challener, and Cheng does not disclose a "second processor configured

to… perform a secure backup of the record to a storage service."

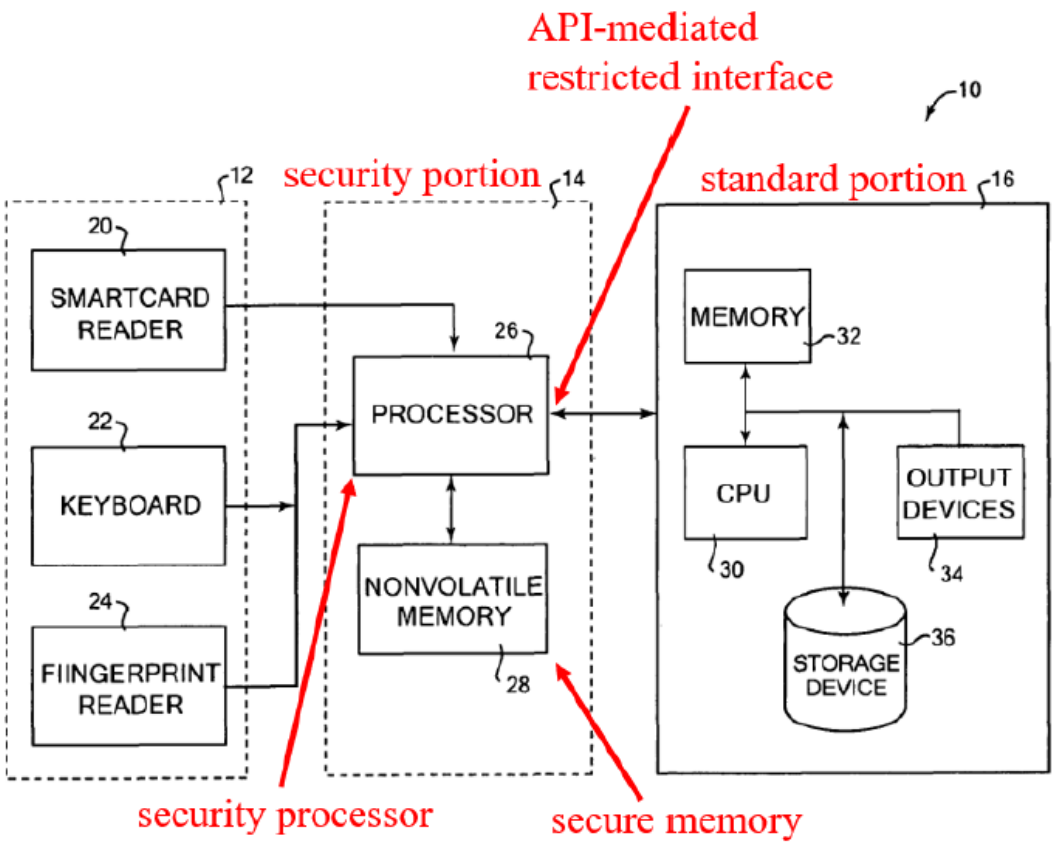
2. A POSITA would not have reasonably expected Cheng to work with the Kesanupalli and Challener combination

70. Petitioner has not shown a POSITA would have had a reasonable expectation of success when combining the combination of the Kesanupalli reference and the Challener reference with the Cheng reference. The only reason Petitioner offers that a POSITA would have had a reasonable expectation of success in combining Cheng with the combination of Kesanupalli and Challener is the following:

> "Adding a backup feature would merely have been applying a known technique to a known device (method, or product) ready for improvement to yield predictable results." Petition at 26.

71. However, TPM access is restricted to prevent unauthorized access and protect TPM data. Petition at 36. That purported reason does not consider or explain at all how the backup would be combined with the TPM and sensor. There is no connection at all between the backup service and the combination of the TPM and sensor. Petitioner provides no explanation as to how the TPM of Challener and the sensor of Kesanupalli could maintain restricted access while simultaneously being able to communicate with and beyond the Host PC, like with the backup storage

service. Even accepting Petitioner's argument that a POSITA would add Challener's TPM to Kesanupalli (which is unsupported and contrary to the understanding of a POSITA), one the main purposes of a TPM is to isolate sensitive information whereas (absent using the '512 Patent as a guide in hindsight) a POSITA would understand that sending the contents of a TPM's secure memory directly to a backup server could be a security vulnerability. Thus, Petitioner's omission is a glaring, because it is very difficult to maintain a TPM's high level of security (that is tied to its isolation) while simultaneously communicating its sensitive contents to a backup storage service that is inherently not isolated. Creating a system that would address these issues would be a monumental task absent the teachings of the '512 Patent itself. Critically, Petitioner has not shown this could be done, let alone with a reasonable expectation of success.



APPL-1007, FIG. 1, annotated

Petition at 14.

3. Dependent Claims 2 and 12

72. Claim 1 requires that "the second processor is configured to… perform a secure backup of the record to a storage service." Further, Claim 2 requires "the storage service comprises a cloud storage service." Claim 12 is similar to claim 2 but depends on claim 11's method.

73. As discussed with regards to claim 1 above, the combination of the

Kesanupalli reference's sensor with the Challener reference's TPM only connects to the Host PC through an SSL connection. As discussed above, the combination of the Kesanupalli reference's sensor with the Challener reference's TPM cannot "perform a secure backup of the record to a storage service." Furthermore, that combination cannot "perform a secure backup of the record to" an internet-based storage. This is because, as discussed above, the internet-based storage service can only communicate with the general processing portion of the Host PC and cannot communicate with the TPM and sensor combination. Accordingly, the Kesanupalli reference's sensor with the Challener reference's TPM is not a second processor that "perform[s] a secure backup of the record to" an internet-based storage.

4. Independent Claims 11 and 21 and Dependent Claims

74. Other than the preambles, claims 1, 11, and 21 are similar. Petition at 71. The Petitioner also claims "[d]ependent claims 12–16 and 20 are substantively identical to claims already addressed." Petition at 69. For the reasons discussed above, these similar claims are not invalidated.

IX. CONCLUSION

75. For the reasons discussed above, it is my opinion that all Challenged Claims of the '512 Patent are valid.

Dated: October 8, 2024

By:

Michael T. Goodrich, Ph.D.

Carbyne Ex. 2037, p.48 of 48
Apple v. Carbyne
IPR2024-00332