EX 1003

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Fortinet, Inc.,

Petitioner,

v.

Netskope, Inc.,

Patent Owner.

Case No. 2026-0040

U.S. Patent 8,356,336

DECLARATION OF DR. JOHN BLACK, JR.

I, John Black, Jr. declare as follows:

I. INTRODUCTION

1. I have been retained on behalf of Fortinet, Inc. ("Petitioner") to provide analysis and opinions regarding the patentability of certain claims in U.S. Patent No. 8,356,336 ("the '336 Patent").

2. I am being compensated for my time at the rate of $675 per hour. I have no interest in the outcome of this proceeding and the payment of my fees is in no

way contingent on my providing any particular opinions.

3. If requested, I am prepared to explain (in a deposition or at a trial before the Patent Trial and Appeal Board (the "Board")) the technology disclosed in the '336 Patent—including the state of the art in the relevant timeframe.

II. EDUCATIONAL AND PROFESSIONAL BACKGROUND

4. My qualifications can be found in my Curriculum Vitae (attached as Appendix A), which includes my detailed employment background, professional experience, and list of technical publications and patents.

5. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now “California State University, East Bay”) in 1988. I received an M.S. in Computer Science in 1997, and a Ph.D. in Computer Science in 2000, both from the University of California at Davis.

6. I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications, primarily on issues relating to computer security. I have been involved with computers and networking for over 40 years in both commercial and academic capacities.

7. My earliest interest was in networks and security. My first memories

in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available, and I spent most of my free time studying, programming, and modifying them. I worked extensively with various networking products throughout the 1980s, and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer Science and Mathematics because cryptography is a blend of these two subject areas.

8. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp as a software developer, writing and reviewing code written in C. My work primarily was directed at transaction logging, data type support, and security.

9. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security and my research involved encryption, authentication, hash functions, and network security.

10. After graduation I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, STP, IP, UDP, TCP, HTTP, SMTP, BGP and other protocols. In 2001, as a graduate student and I looked at the security of ARP and invented a new protocol "AuthARP" to add security to the protocol.

11. In 2002, I moved to the University of Colorado at Boulder where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new course called "Foundations of Computer and Network Security," which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services including the world-wide web. I have taught this class seven more times since then, including modern topics such as wireless networking, the Internet of Things, and so forth.

12. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several PhD students in these areas.

13. I have also worked for a consulting company at times, writing software on contract basis. Although most projects are covered by NDAs, many involved networks and/or aspects of computer security.

14. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM, but also has included networking projects and embedded device work. For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App, worked on

802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop. My work has been adopted into various commercial protocols, including enterprise Wi-Fi and EMV tap-to-pay technology.

15. As part of my duties in the Computer Science department at the University of Colorado I served as chair of the Computing Committee. In 2014, I oversaw the construction of a new datacenter, including cooling, power conditioning, cabling, networking, and security for the research units within the department.

16. In 2016, I took a two-and-a-half year leave of absence from the University of Colorado to start a company named "SecureSet" in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical people and turn them into computer and network security specialists via five months of intensive training. SecureSet was sold to WeWork in 2019 and continues to offer computer security classes today. In 2018, I returned to my position at the University where I remain employed to the present day.

III. MATERIALS REVIEWED

Exhibit	Description
1001	U.S. Patent No. 8,356,336 ("the '336 patent")
1002	File History of the '336 patent
1004	U.K. Patent Application GB2389010A ("Subbiah")

Exhibit	Description
1005	PCT Publication No. WO 2002/039237 ("Hinton")
1006	U.S. Patent Appl. No. US 2004/0177276 ("MacKinnon")
1007	Crandell et al., *A Secure and Transparent Firewall Web Proxy* ("Crandell")
1008	Bauer et al., *Designing and Using DMZ Networks to Protect Internet Servers* ("Bauer")

17. In preparing this declaration, I reviewed and considered the above materials, along with any other materials referenced in the body of my declaration. I may use these documents and information, or other information obtained during the course of this proceeding, as well as representative charts, graphs, schematics and diagrams, animations, and models based on those documents and information, to support and to explain my testimony.

18. My opinions are based in part on a review and analysis of the abovementioned documents and materials. I have also drawn on my education, experience, and knowledge of basic engineering and design principles in forming my opinions.

IV. RELEVANT ART AND LEVEL OF ORDINARY SKILL

19. I have been informed that the level of ordinary skill in the relevant art at the time of the invention is relevant to inquiries such as the meaning of claim terms, the meaning of disclosures found in the prior art, and the reasons one of ordinary skill in the art may have for combining references.

20. I have been informed that factors that may be considered in determining

the level of ordinary skill include: (1) the type of problems encountered in the art; (2) prior art solutions to those problems; (3) rapidity with which innovations are made; (4) sophistication of the technology; and (5) education level of active workers in the relevant field. I have been further informed that a POSITA is also a person of ordinary creativity.

21. In my opinion, A POSITA in the field of the '336 Patent would have had either (1) at least a bachelor's degree in computer science or computer engineering or an equivalent field plus at least one year of experience working on computer networking or computer security, or (2) at least 3 years of experience working on computer networking or security, even without a formal degree.

22. At the time of the alleged invention, I was at least a POSITA in the art relevant to the '336 Patent. Further, based on my experience, I understand and know of the capabilities of a POSITA in 2004—and I am familiar with how a typical POSITA would have understood and used the terminology found in the '336 Patent and the Challenged Claims at the time of filing, and with the state of the art at that time.

23. Even though my own experience and qualifications exceed that of a POSITA, the statements herein regarding the knowledge of a POSITA and what would have been obvious to a POSITA are from the perspective of POSITA at the relevant priority date.

V. LEGAL STANDARDS APPLIED

24. I am not an attorney, but I have been informed of several legal principles, which I have employed in forming my opinions in this declaration. I have been informed that each patent claim is considered separately for purposes of patentability and that a dependent claim that depends from another claim includes all of the limitations of the claim from which it depends.

A. Burden of Proof

25. I have been informed that the petitioner in an *inter partes* review bears the burden of establishing unpatentability by "a preponderance of the evidence." I have been further informed and understand that, to prove an assertion by "a preponderance of the evidence," the party with the burden of proof must demonstrate that it is more likely than not that the assertion is true.

B. Claim Construction

26. I have been informed that the claims of the '336 Patent in this proceeding are to be construed using the same claim construction standard applied in district court. I have been informed the claim construction analysis begins with the ordinary meaning of a claim term, and there is a presumption that the term carries its plain and ordinary meaning to a person of ordinary skill in the art ("POSITA") as of the effective filing date of the patent. I have also been informed that the most important sources for determining the meaning of a claim term are the claims, the specification, and the prosecution history of the patent at issue, which collectively is

"intrinsic evidence." I have also been informed that a patentee can act as their own lexicographer and provide specific definitions of claim terms that may differ from the plain and ordinary meaning.

1. "shared network"

27. A POSITA would have understood "shared network" in the context of the '336 patent to mean "a local network to which an unauthenticated user has access." This is based on the patent's stated purpose of facilitating network access control for a user—such as a wireless device user—at a local area network. *See, e.g.*, EX1001, 1:34-62. As the patent explains, a user signing on to the local mall's wireless network may be provided free access to the local network but may require additional authentication to get access to an external network, such as the Internet. *Id.* But in describing the servers to which the wireless user is provided access without authentication, the specification makes clear it is for *local* servers—*i.e.*, "the Web server for the mall, plus one or more other Web sites that are associated with the mall (*e.g.*, the ***local Web server*** for a tenant in the mall, such as a department store or movie theater." *E.g.*, 1:39-47.

2. "anonymous user"

28. A POSITA would understand the term "anonymous user" as used in the claims of the '336 patent to refer to a user unknown to the system in the sense that the user is unauthenticated. For example, element [1b] recites the network access

controller intercepting "a request to access a network resource from a browser application running on a client device within the shared network associated with an anonymous user" but does not otherwise define the "anonymous user." EX1001, claim 1. In addition, element [1e] specifies that "the anonymous user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network without authentication."

29. This is consistent with the specification's disclosure that the "anonymous user on a different Client would still be restricted to the Walled Garden," while the "authenticated user" is granted "external" access (e.g., to the Internet). EX1001, 5:36-39; *see also* 4:50-60 (teaching "anonymous user has access to one of the Client network access devices" and "the anonymous user may access Web locations on any of the three servers that are in the Walled Garden 5"). This understanding is also supported by Figure 3 which shows that a user who is not authenticated is restricted to the walled garden unless subsequently authenticated. EX1001, FIG. 3, 5:45-6:16.

3. "pre-authentication capture destination"

30. A POSITA would understand the term "pre-authentication capture destination" to refer to any pre-defined destination within a closed network. Here the word "capture" refers to the "captive portal" confining pre-authenticated users to the local network, or "walled garden." An example of a pre-authentication capture

destination would be a web page hosted within the confines of the walled garden.

31. The understanding is confirmed by the specification teachings that "[e]mbodiments disclosed herein enable a public/private network service provider to automatically redirect anonymous clients to a pre-defined destination within a limited set of network destinations." EX1001, 2:47-50; *see also* EX1001, 2:53-59 ("they will be redirected to the pre-defined destination"). The '336 patent specification further explains that the "Pre-Authentication Capture Destination" can be a Web page hosted on a local server. E.g. EX1001, 4:50-62 (the method can include sending "an HTTP redirect to the Client's browser, specifying the Pre-Authentication Capture URL 'http://wg1.com/welcome.html'. The browser then automatically performs an HTTP Get to retrieve that Web page from the wg1.com server."). As the specification also teaches, "[a]ny attempt by an unauthorized client to access a network resource that is not in …the list of servers that make up the 'walled garden'[] will result in the client being re-directed…to the Pre-Authentication Capture Destination" and "[a]ny attempt to access a website…that is outside of the walled garden will cause the client to be re-directed back to the Pre-Authentication Capture Destination." EX1001, 2:7-19.

4. "authentication token"

32. A POSITA would understand "authentication token" as used in claims 5-7, 12-14, and 19-20 to refer to a unique sequence of characters for use within the

query portion of a URL (*e.g.* so as to pass information between a client and network devices) that may be used to redirect a client to an authentication screen. For example, in claims 5-7, the patented method looks for the presence of an "authentication token" but does not use or process that token beyond making a yes or no determination of whether that token is present. *See* EX1001, Claim 5 ("method according to claim 1, further comprising: … determining whether the second request contains an authentication token."), FIG. 3 (step 23, "URL contains authentication token?"), 6:3-5 ("the Network Access Controller 2 determines if the packet contains the Authentication Token (step 23)."). "If…the packet does not contain the Authentication Token, then the Network Access Controller 2 directs the client to the Pre-Authentication URL (step 25)." EX1001, 6:6-11. However, if "the packet contains the Authentication Token, then the Network Access Controller 2 directs the client to the Authentication URL." EX1001, 6:12-16. A POSITA therefore would have understood that the '336 patent claims care only whether the token is present of absent, but the specific contents of the token are unimportant to the claims. This is consistent with the specification's description of the token, explaining that the term "authentication token", as used in the patent, simply refers to "a unique sequence of characters that are valid for use in the query portion of a URL." EX1001, 2:30-34. The specification makes clear that "the exact form of this special token need not be predefined; the special token is simply uniquely identifiable." EX1001, 5:11-16.

33. For all other terms in the '336 Patent, I have performed my analysis using their plain and ordinary meaning to a POSITA.

C. Anticipation

34. I have been informed that a patent claim is unpatentable if it is "anticipated" by prior art. I have been informed that a reference anticipates a claim if the reference discloses each limitation of the claim at issue, either expressly or inherently. I have been informed that a prior art reference may anticipate a claim without disclosing a feature of the claimed invention if that missing characteristic is necessarily present, or inherent, in the single anticipating reference as would have been understood by a POSITA.

D. Obviousness

35. I have been informed that a patent claim is unpatentable if it would have been obvious to a POSITA at the time of the claimed invention. I have been further informed that a claimed invention is not patentable if differences between it and the prior art are such that the subject matter as a whole would have been obvious to a POSITA at the time of invention. I have been informed that factors relevant to the determination of obviousness include the scope and content of the prior art, the level of ordinary skill in the art at the time of the invention, differences between the claimed invention and the prior art, and "secondary considerations" or objective indicia of nonobviousness.

36. I have been informed that a single reference alone can render a patent claim obvious if any differences between the reference and the claim would have been known or obvious to a POSITA at the time of the invention. That is, if the POSITA could have adapted the reference to meet the claims of the patent by applying known concepts to achieve expected results, then the patent claims are rendered obvious by that reference.

37. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I have been further informed and understand that when a patent claim simply arranges old elements with each performing the same function it had been known to perform and yields no more a POSITA would expect from such an arrangement, the combination is obvious.

38. I have been informed that a patent claim composed of several limitations is not obvious merely because each limitation was independently known in the prior art. Hindsight reasoning is not an appropriate basis for combining references to form an obviousness combination. I have been further informed that it can be important to identify a reason that would have prompted a POSITA to combine multiple prior art references, or multiple teachings of the same prior art reference.

39. I have been informed that various "secondary considerations"

(sometimes referred to as objective indicia of nonobviousness) may support a determination of nonobviousness and that such secondary considerations must be considered as part of an obviousness analysis. I have been informed that even strong evidence of secondary considerations may not be sufficient to rebut a strong showing of obviousness. I have been informed that the patentee bears the burden of showing the existence and effect of secondary considerations of nonobviousness, after which the burden of coming forward with rebuttal evidence shifts to the party arguing obviousness. I have been informed that the following secondary considerations may indicate nonobviousness:

a. Evidence that others, including the accused infringer, copied the patented invention.

b. Evidence of a persistent problem or need in the art that was resolved by the patented invention.

c. Evidence that others have tried and failed to solve the problem or failed to provide the need resolved by the claimed invention.

d. The willingness of industry to license the patent at issue.

e. Evidence that those of ordinary skill in the art were skeptical as to the merits of the invention.

f. Evidence of praise directed to the invention by others in the field.

g. Evidence that those of ordinary skill in the art were surprised by the capabilities of the claimed invention.

40. I have also been informed that the near-simultaneous invention by others can be evidence that a claimed invention is obvious.

41. I have further been informed that the patentee bears the burden of showing a "nexus" between the claimed invention and the evidence proffered on secondary considerations.

VI. TECHNOLOGY BACKGROUND

42. The '336 Patent deals with general networking concepts and systems that were well know and well understood as of 2004.

Overview of the Internet

43. The Internet is a global network of millions of devices. In reality, it is comprised of a large number of smaller networks that are all interconnected. Its workings are vastly complex; I will give a high-level overview of how it functions, doing my best to simplify the exposition to make an understanding the main ideas more accessible.

Linking Devices Together

44. Every device on the Internet can, in theory, connect to any other. In order to achieve this, there must be a series of links along which information can travel from one point to another. These links can take many forms: a fiber optic link, a coax cable, a copper wire, a satellite link, a cellular link, etc. One principal design

goal of the Internet is that it can operate across a wide variety of link-types, and its success in *achieving* this is one of the reasons for the Internet's overall success.

45. Signals across all of these links occur as electromagnetic waves in various portions of the electromagnetic spectrum. These waves may operate as radio waves (through the air or inside of a wire), as optical light, or in other spectra such as infrared or microwave. All of these are part of the radio frequency spectrum and therefore communications encoded using these technologies constitute electromagnetic communications.

IP or the "Internet Protocol"

46. The Internet is a packet-switched network. All packets sent and received over the Internet are transmitted using the Internet Protocol (or "IP")[1]. In order to use the IP protocol, information is broken up into manageable chunks called "packets" and then transmitted over the various links from one device to another.[2]

47. The IP protocol is "best effort" meaning that there is no guarantee that a particular packet will actually reach its intended destination. There are many reasons that a packet could be lost: transmission error, packet corruption, saturation of a given link, and other kinds of failures could cause a packet to be lost in transit.

IP Addresses

---

[1] By "IP" we mean "Internet Protocol version 4" or "IPv4" which is the format for the vast majority of Internet traffic over the last twenty years.

[2] *See, e.g.*, FRC 791 available at https://datatracker.ietf.org/doc/html/rfc791.

48. In order for a packet to be sent from one device to another using the Internet, each must have a globally-unique IP address.[3] An IP address is comprised of four numbers between 1 and 255, usually written with a period separating them. For example,

23.66.124.110

is a valid IP address written in the standard format. In fact, this address belongs to the U.S. White House.

49. Every device connected to the Internet must have an IP address.

Domain Name Service (DNS)

50. Although computers are efficient at processing information based on numbers like IP addresses, we humans often prefer more descriptive names. Instead of trying to remember the White House's IP address, 23.66.124.110, most of us would prefer www.whitehouse.gov as the website for the White House. We therefore require a service that can translate between these two designations efficiently: given a "domain name" like www.whitehouse.gov we should be able to find its IP address, and given 23.66.124.110, we should be able to recover its domain name. The service

[3] This is once again an oversimplification. The world has run out of IP addresses and therefore we use tricks in order to allow multiple devices to share a single IP address. This would be analogous to a street running out of available addresses, and then instituting "apartment numbers" as a way to allow distinct dwellings to share a given street address provided they have different apartment numbers.

that provides this translation is called the Domain Name Service (or "DNS").[4]

51. As stated above, every computer on the Internet *must* have a numeric IP address, but having a DNS name is *optional*: indeed, most computers on the Internet do not have one.

HyperText Transmission Protocol (HTTP)

52. Web-based communication is commonly conducted using a protocol called the "HyperText Transmission Protocol" or "HTTP" sent over TCP/IP between a browser and a web server.[5] Although in recent years HTTP has evolved to use UDP/IP (an alternative to TCP/IP), in 2004 the prevalent version of HTTP was 1.1 and that version used TCP/IP exclusively. I will assume HTTP version 1.1 for the purposes of this declaration.

53. The most common HTTP request from a browser is a "GET request" which is a request in plain text that starts with the word "GET" followed by a URI naming the requested resource, followed by "HTTP/1.1" indicating the version. Consider the following example for a user on the Internet who types the web site of my employer into her browser bar, "www.colorado.edu".

54. First her browser would perform a DNS lookup to translate the name "colorado.edu" into an IP address. Next the browser would connect to that IP

[4] *See, e.g.*, RFC 1035, available at https://datatracker.ietf.org/doc/html/rfc1035.
[5] *See, e.g.*, RFC 1616, available at https://datatracker.ietf.org/doc/html/rfc2616.

address using TCP/IP. Then the browser would send something like "GET http://www.colorado.edu/index.html HTTP/1.1" through the established connection[6]. This message is the first appearance of the HTTP protocol in this session. The web server would then respond with an HTTP response followed by the contents of the University home page, expressed in HTML which the browser would then render.

55. A GET request can also include parameters, which are additional pieces of information appended to the URL that the server may then react to appropriately. For example, if my university had a web form that asked for my zip code, and I filled in this form and clicked on a "Submit" button, the resulting GET request might look like this:

GET http://www.colorado.edu/showmap.html?zipcode=80027

56. Here the location of the web resource ends at the "html" portion, and the remainder beginning with the question mark indicates the start of supplemental parameters.

57. If the website owner wishes to redirect traffic to a different website, HTTP supports the concept of a "redirect." This is often done by returning a "301

[6] In 2025, virtually every website requires encryption meaning further steps would be required to set up a TLS connection. In 2004 this was far less common and in my present example, I am not using TLS.

response” with a Location header indicating where the browser should be redirected. Virtually all browsers will automatically process a 301 response by fetching the indicated URL from the Location header without user interaction. For example, a website could respond to a GET request with

```
HTTP/1.1 301 Moved Permanently
Location: https://www.example.com/new-page
Content-Type: text/html; charset=UTF-8
Content-Length: 0
```

58. The above header fields would then be followed by a blank line and then the body of the response (if any).

Cookie

59. A “cookie” is a string of information (*i.e.*, a collection of letters and digits) that is sent by a particular web site to the browser with the understanding that the browser will store the cookie in its storage facility (often called a “cookie jar”) and then remit that information back to the server upon all subsequent visits. Some limitations can be imposed, and cookies can be given an expiration date after which they are deleted.

60. The browser works as follows: if a given web site is to be accessed (either by user direction or by automated means) the browser searches its cookie jar and looks for any cookies associated to the URL being accessed. Any matching cookies are then added to the “cookie” header field in the request before the HTTP request is transmitted to the corresponding web server. This mechanism provides an

easy way for web sites to keep track of users which would otherwise be difficult (web sites often handle scores of users simultaneously, and thus they need to be able to differentiate between users reliably). Once use of cookies is to indicate that a user has successfully logged in by presenting her username and password; the web site, in order to remember this user's status, will set a cookie in her browser that uniquely identifies the session; these are often called "session cookies." Another use of cookies is to track users in order to study or trace their behavior (*e.g.*, for advertising purposes); these are sometimes called "tracking cookies."

Captive Portals

61. Most users will be familiar with the experience of taking a mobile device (phone, tablet, laptop, etc.) to a new location that has WiFi Internet available. After connecting a device to a WiFi access point, a user might be redirected to a special "landing page" that requires agreeing to the "terms of use" for the network, displays ads, requires payment, or other requirements that are prerequisites before permitted the user to access the full Internet. If the user does not comply with the requirements, she is denied access to the full Internet; in some instances she may still be able to have limited web access to a restricted set of sites. The restricted network is often called a "restricted network" or a "walled garden."

62. The technology above as a whole is often called a "captive portal." This reflects the notion that the user is "captured" by the WiFi access point "portal" and

held until various requirements are met. Although today, the redirection happens automatically in most cases (Google, Apple, and Microsoft all have dedicated redirect URLs to enable their various products to be auto-redirected), in 2004 this was not the case. Instead, the following was usually the technology used:

- The user connects to WiFi and issues a DHCP request, looking to be assigned an IP address, gateway address, and address of the DNS server
- The captive portal responds with a local IP address assignment, the gateway address, and the DNS server of the captive portal itself
- The user types in a URL into her browser and the browser does a DNS lookup
- The captive portal DNS server resolves to the address of the landing page of the captive portal, no matter what the user typed in
- If the user complies with all requirements, the DNS server then responds properly from that point forward

63. The only step above that differed in 2004 from today was the requirement that the user attempt web access to trigger the captive portal instead of automatic triggering as is common today. Back in 2004, an attempt to start with a TLS site would break the captive portal and just cause the system to hang, so users had to know to go to a non-TLS site (such as neverssl.com). All of this has been

fixed in 2025.

64. Once a user has been authenticated, she has full Internet access. The access is usually enabled by the captive portal recording the MAC address of the authorized device for some duration, which will eventually expire.

VII. THE '336 PATENT AND PROSECUTION HISTORY

A. The '336 Patent

65. The ’336 patent describes techniques for managing client access within a network environment that includes both private (local) and public (external) domains. See EX1001, 1:25–38. As described in the specification, one contemplated use case involves a shopping mall operator providing wireless access to on-site customers. The shopping center's users may be permitted to access a locally-hosted web server containing the mall’s website and other affiliated content. See EX1001, 1:39–44. The specification refers to this restricted set of accessible resources as a “walled garden.” See EX1001, 1:44–47. While any users of the local network may be able to access locally-stored content, only properly authenticated users may be granted access to the public Internet. See EX1001, 1:48–55.

66. The purported innovation in the independent claims lies in the redirection of attempts to access the public network by unauthenticated clients within the shared network to a designated internal destination—the “Pre-Authentication Capture Destination.” This location, such as a welcome screen,

serves as an entry point within the walled garden. See EX1001, 1:66–2:19. In contrast, authenticated users are not redirected but are permitted to access external network resources directly. See EX1001, 5:24–39. According to the specification, unauthenticated users are limited to the walled garden; any attempt to access a resource outside of it results in redirection to the capture destination. See EX1001, 2:13–18.

67. Dependent claims, such as claims 5, 12, and 19, introduce the concept of an “authentication token” used to identify whether a client request should trigger an authentication process. As disclosed, the token is a unique character string embedded in the request—typically within the HTTP URL. Detection of this token by the Network Access Controller causes the client to be redirected to an authentication interface rather than the default capture page. See EX1001, 2:31–40.

68. The patent illustrates its system in Figures 1 and 2. In Figure 1, the client device is connected a "Network Access Controller" and, through the Network Access Controller, to the Walled Garden. EX1001, FIG. 1, 3:1-6 (Figure 1 shows "network access capability afforded to an unauthenticated client"). In Figure 2, the client device is still connected to the Walled Garden, but the Network Access Controller has also granted it access to the Internet. EX1001, FIG. 1, 3:1-6 (showing "network access capability afforded to an authenticated client").

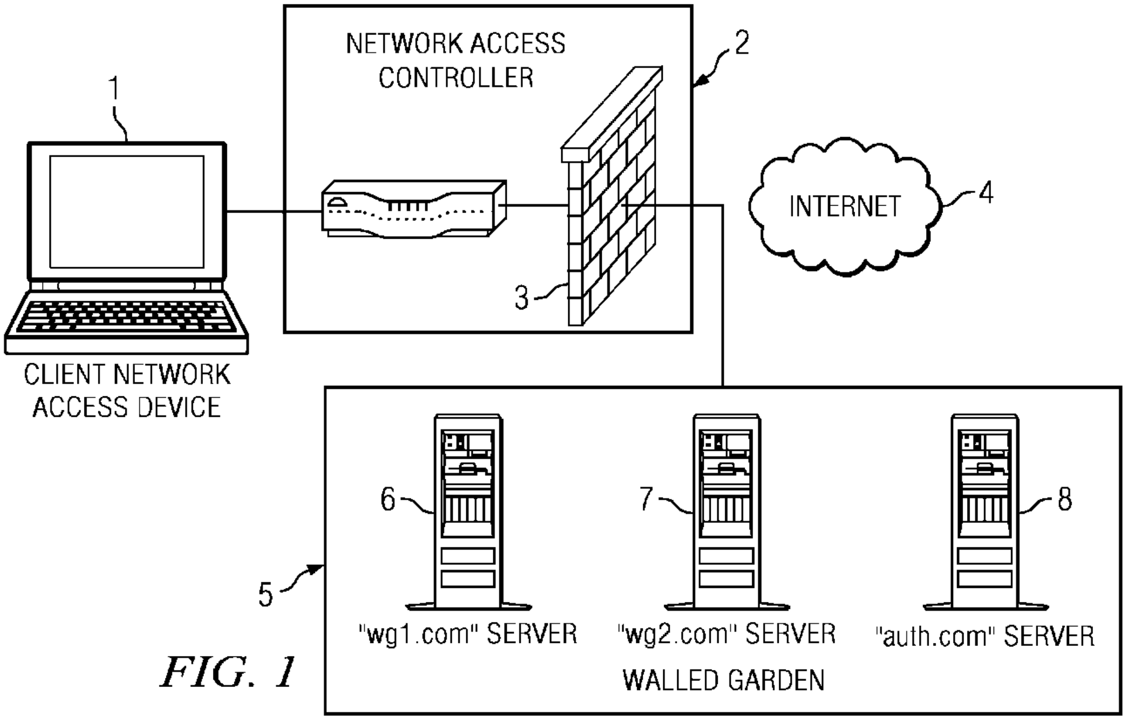


FIG. 1

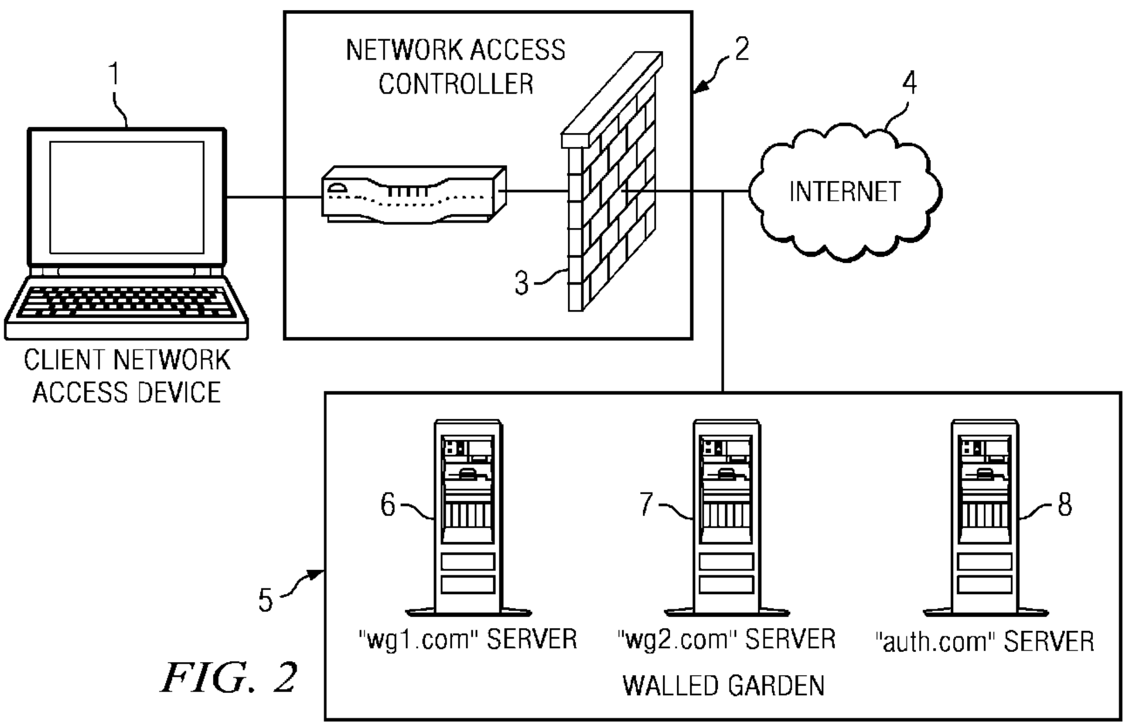


FIG. 2

69. The process claimed by the '336 patent is described in Figure 3, which

includes four different determinations that the network access controller uses to control access to the Internet and re-direct users.[7]

(1) Is the user authenticated? (Step 20)

(2) Is the destination local (*i.e.*, in the walled garden)? (Step 21)

(3) Is the destination a URL? (step 22)

(4) Does URL have a token? (step 23)

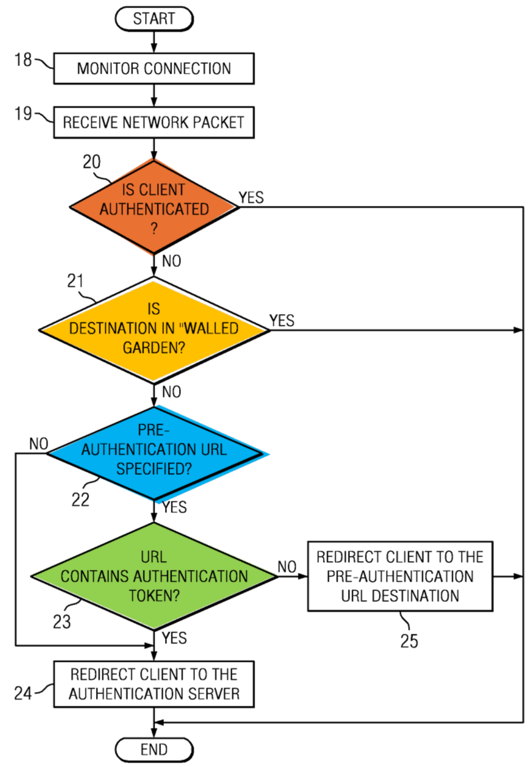


FIG. 3

70. As Figure 3 illustrates, the authenticated client is granted access to all resources. EX1001, 5:45-50, FIG. 3. If not authenticated, the client still has access to all destinations within the walled garden. *Id.*, 5:51-58; FIG. 3. If the user is unauthenticated (*i.e.*, "anonymous"), then the network access controller checks to see if the URL specified was the pre-authentication URL; if not then the user is sent

[7] I note, however, that not all four steps are required by each Challenged Claim. For example, Step 23 (checking for an authentication token) implicates only a subset of the dependent claims.

directly to the authentication login screen. (steps 22, 24)[8]. But if the user does specify the pre-authentication URL then, in the flowchart of Figure 3, the controller checks if the URL includes an authentication token (or flag) indicating that the user should be redirected to the authentication login screen. (step 23). If the URL includes the flag, the user is redirected to the login screen; if the URL does not include the flag, then the user is redirected to the "pre-authentication URL destination." EX1001, 5:59-6:11.

B. The '336 Prosecution History

71. I understand that the ’336 patent originated as U.S. Patent Application No. 12/619,560, filed Nov. 16, 2009. I further understand that the '336 patent claims priority to U.S. Provisional Application 60/551,705 (filed 3/10/2004), and U.S. Provisional Application 60/551,702 (filed 3/10/2004).

72. Originally filed claims 1-6, 9-13, and 16-19 were rejected as obvious over two non-patent references, Crandell et al. ("A Secure and Transparent Firewall Web Proxy") (EX1007) and Bauer ("Designing and Using DMZ Networks to Protect Internet Servers") (EX1008), which the Examiner identified as disclosing interception and redirection of unauthenticated requests for access. EX1002, pp. 165-167. Likewise, the Examiner also identified determining whether a "request includes an authentication token (i.e., determining whether the second request

[8] I note that Step 22 of this process is not claimed in the '336 patent claims.

contains a cookie)" and redirecting a browser based on the presence (or absence) of that cookie as already within the prior art. *Id.* In response to the Examiner's rejection, the Applicant amended the claims to specify that the client device accessing the local area network must be "within the shared network." EX1002, p. 218. I understand that, based on this amendment, the Examiner allowed the Challenged Claims, stating "[t]he closest prior art, MacKinnon et al. (US2004/0177276), also discloses redirecting a client's request to a pre-authentication capture destination; however, MacKinnon does not disclose that the pre-authentication capture destination is hosted on a first server in the shared network." EX1002, p. 240.

VIII. PRIOR ART

A. GB2389010 to Subbiah (EX1004, "Subbiah")

73. Subbiah is a UK patent application, published as GB2389010 on November 26, 2003. Subbiah was filed March 26, 2003. I understand Subbiah is prior art to the '336 patent.

74. Similar to the '336 patent's public/private network set up, for example, in a shopping mall, Subbiah discloses a wireless access point that "provid[e] communications network access (e.g., Web page browsing, instant messaging, e-mail, etc.) in a public area (e.g., a mall, airport, sports arena, etc.)." Subbiah, 4:12-15. Subbiah's network includes a "local domain of the communications network,

such as, for example, a local Intranet of a shopping mall, airport, or the like" and an external domain, "outside the local domain, such as, for example, popular sites or Web pages on the Internet." Subbiah, 4:18-24.

75. Subbiah's discloses a client device connected both to a local domain and to an external domain (such as the Internet) through a wireless access point. FIGs, 1, 3. Users are given different levels of access based on authentication and the appropriate permissions. Subbiah, 14:17-24. ("wireless access point 330 is configured to provide different levels of access to services" including local network access, web and telnet access and "full" access). Subbiah's "wireless access point" is described as intercepting and redirecting network requests from a client and therefore is a network access controller, as claimed in the '336 patent. *E.g.*, Subbiah, 15:9-12, 16:2-8.

76. And like the '336 patent, Subbiah's wireless access point controls network access using the same four basic determinations:

(1) Is the user authenticated? (Step 703)

(2) Is the destination local (*i.e.*, in the walled garden)? (Step 704)

(3) Is the destination a URL? (*i.e.*, is the client "using a Web browser" (Subbiah, 17:18-22) (step 706)

(4) Does the URL have a token? (*i.e.*, is it a "first time request") (step 707)

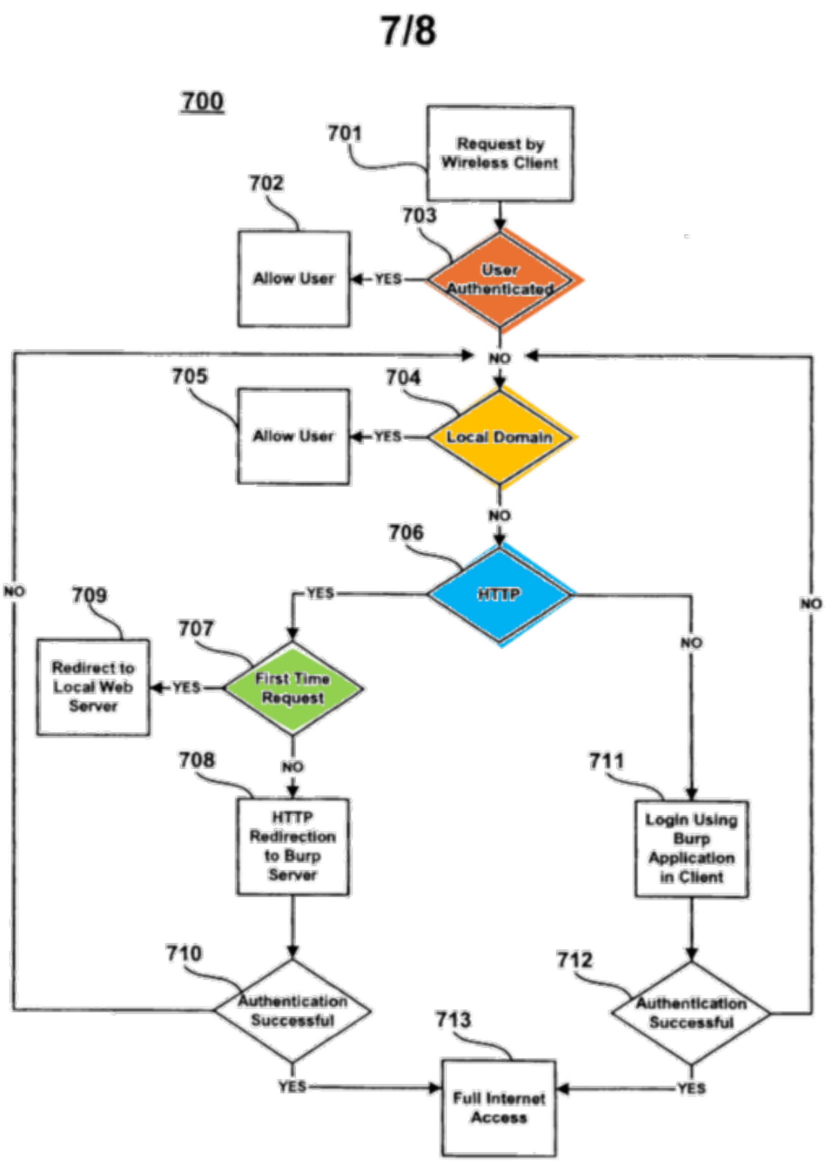


FIG. 7

77. Subbiah's Figure 7 flowchart highlights that the two methods are virtually identical in all relevant ways. First, an authenticated client is always given

full network access, including to the Internet. Subbiah, 17:10-14, FIG. 7 (steps 702, 703). Second, an unauthenticated client is permitted access to any resource within the walled garden. *Id.*, 17:16-18; FIG. 7 (steps 704, 705). Third, if the unauthenticated user uses a URL (i.e., requests an Internet HTML page using HTTP), then the system checks for some indication (e.g., a flag) as to whether it's a first time request or not. Users will be redirected either to the "Local Web Server," and in particular to a "main, or default, Web page 400," (*i.e.*, the "Pre-Authentication Capture Destination") if the user requested an Internet HTML page (e.g., using an HTTP URL), or to the authentication server (because some flag indicates it is not the user's first visit or the user is not requesting a URL). *Id.*, 15:7-13, 16:2-14, 17:18-18:4, FIG. 7 (steps 706-709, 711). Finally, "in the event of an unsuccessful authentication process" the user is "provide[d] access to the information and services of the first area" (*i.e.*, the local domain). 13:14-17, FIG. 2.

78. With respect to the determination of step 707—checking whether it is the user's "first time request," a POSITA would have understood, or at minimum found it obvious, to use tokens (such as a flag or a cookie) within the request to quickly and easily transmit state information between the client and access point. This is because in 2004 (and to the present day), it was common to pass "state" information between a client and server either as a URL parameter (*i.e.*, a parameter

sent as a "query string parameter" in a GET request[9]) or in a header field for a GET or POST request, such as via a cookie[10].

79. Similarly, to the extent PO argues that Subbiah Figure 7 is silent as to what happens when authentication fails, a POSITA would have understood Subbiah to disclose, or at minimum render obvious, that the access point would redirect the unauthenticated client back to the "main" Web page on the local server. This is evident from the flowchart of Figure 2—a simplified version of Figure 7—which teaches that "in the event of an unsuccessful authentication process as determined in step 204, process 200 proceeds to step 206 and provides access to the information and services of the first area". Subbiah, 13:14-17. This behavior was common in 2004, and is common today when authentication attempts fail; for example, when logging into a web site, most users are familiar with the behavior evident when mistyping their password: the web site redirects the user back to the same login screen once more.

B. WO 2002/0339237 to Hinton (EX1005, "Hinton")

80. Hinton is a PCT Patent Application published as WO 02/39237 on May 16, 2002. Hinton was filed October 25, 2001 as PCT/EP01/12361. I understand that

[9] Query string parameters are described in RFC 2396, published in August 1998; see https://www.ietf.org/rfc/rfc2396.txt

[10] Maintaining session state via cookies is described in RFC 2965, published October 2000; see https://datatracker.ietf.org/doc/html/rfc2965

Hinton is prior art to the ’336 patent.

81. Hinton discloses a system for enabling "cross-domain single sign-on, authentication functionality," by transmitting an "authentication token" between domains using standard "HTTP redirection" techniques. See Hinton, Abstract. As Hinton explains, HTTP redirection was a well-established mechanism in the art:

> "HTTP Redirects are well known in the art. An HTTP Redirect allows a server to respond to a client request with instructions to load a resource at a different location, and in response, most browsers will automatically request the new resource in response to a redirect. When the browser receives the HTTP Redirect, the browser issues a new HTTP Request using the redirected URI provided in the HTTP Redirect." Hinton, p. 24.

82. In the context of accessing a protected resource, Hinton’s server generates an “introductory authentication token” (step 410), appends it to the redirect URI, includes this URI in the HTTP redirect response, and transmits it back to the client (step 412). *See* Hinton, p. 23-24.

83. Hinton further teaches that the authentication token is encoded in ASCII and appended directly to the URI. The browser transparently includes this token in its subsequent HTTP request, without being explicitly aware of its presence or function. *See* Hinton, p. 25-26. In addition, the server is configured to inspect incoming HTTP requests for the presence of an authentication token. If the token is absent, the system triggers a manual authentication workflow. See Hinton, p. 16 (“the server determines whether the client's HTTP Request contains an introductory authentication token, preferably appended to the URI (step 212)... If the HTTP

message does not have an introductory authentication token, then the server forces the user at the client to complete a manual authentication process").

84. Thus, Hinton illustrates a well-known approach in the art for tracking user authentication state using tokens embedded in URIs. More broadly, it was common practice at the time to use such tokens in HTTP requests for conveying client-side state information, including authentication status. A person of ordinary skill in the art would have recognized that incorporating Hinton's authentication token mechanism into Subbiah's access control framework would be both logical and advantageous and would have been so motivated.

85. Hinton and Subbiah and the '336 patent address closely related problems—namely, managing controlled access to network resources in environments that may span multiple domains. *See, e.g.*, EX1001, 1:34–38; Subbiah, Abstract; Hinton, Abstract. Both are directed to access control systems operating over communication networks, making Hinton reasonably analogous art to the '336 patent. *See* Hinton, Abstract.

86. Subbiah's system already includes logic for determining whether a request represents a user's first attempt to access a resource (e.g., step 707 of FIG. 7), and it uses that determination to conditionally redirect the client to either a default home page or an authentication interface. *See* Subbiah, FIG. 7. A POSITA would have found it straightforward to implement this decision point using Hinton's token-

based approach—simply checking for the presence or absence of an authentication token in the URI rather than relying on session tracking or other less explicit mechanisms. This would not only streamline the logic but would also align with well-established practices in HTTP-based authentication systems.

87. In this context, a POSITA would have understood Hinton's disclosures as providing concrete implementation details for redirect behavior already contemplated by Subbiah. The combination would yield a predictable outcome: a functioning access control mechanism using token-based redirection. Given the complementary nature of these teachings, the integration of Hinton's token approach into Subbiah's system would have been an obvious and routine design choice at the time, requiring no inventive insight.

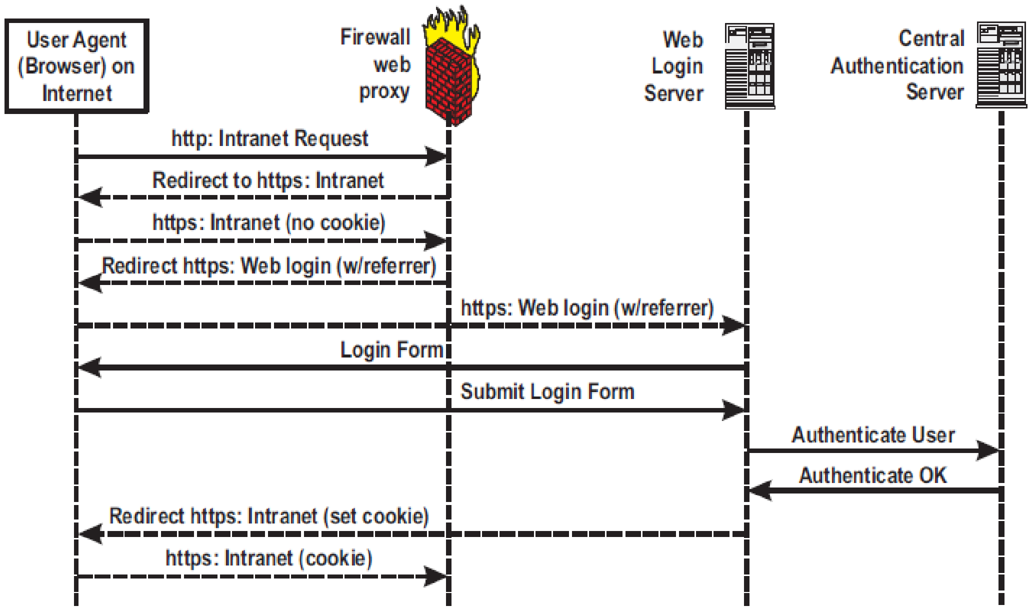
C. Crandell et al., A Secure and Transparent Firewall Web Proxy ("Crandell")

88. I understand from the File History of the '336 patent that PO submitted the publication "A Secure and Transparent Firewall Web Proxy" by Crandell, et al. ("Crandell", EX1007), as prior art to the '336 patent. EX1002, p. 38. As noted on the face of Crandell itself, it was published as part of USENIX Association's Proceedings of the 17th Large Installation Systems Administration Conference. Crandell, p.22. I further understand that Crandell was the subject of multiple rejections by the Examiner with PO never objecting to its status as prior art. *E.g.*, EX1002, p. 165.

89. **Crandell** discusses a "transparent firewall web proxy" designed to "allow[] authorized and secure access to the many firewall-protected intranet web servers at Los Alamos National Laboratory (LANL)." Crandell, p.23. In other words, **Crandell** discloses a way to control access to shared network environments and to ensure that only authorized persons are provided access; in particular, to control "access to intranet web servers from the Internet." *Id.*

90. **Crandell**'s concept is to use "a web authentication system to tell whether or not to forward the User's HTTPS requests." Crandell, p.25. In order to do this, Crandell relies on "cookies" to identify if an access request comes from an already authenticated request or if it needs to be subsequently authenticated: "First the proxy must be able to tell if an HTTPS request comes from an authenticated user session. Second, if the HTTPS request does not include valid authentication credentials, the proxy needs the URL of a web site that handles an initial, interactive user login." *Id.* As Crandell further explains, a "popular method[] for keeping track of authenticated web sessions" uses "cookies" *Id.* (citing RFC 2965). "The cookie string…contains no intrinsic value or information beyond bearing reasonably unique…" and "[e]very new HTTPS request causes the cookie to be re-verified." *Id.* **Crandell** further discloses using these cookies in an implementation scheme relying on "iptables redirect" rules. Crandell, p.26. Figure 4 of **Crandell** discloses such an implementation with cookies being transferred back and forth as part of the HTTPS

requests.



Note: Dashed lines are the result of redirects
Figure 4: Initial HTTP request.

91. The Examiner expressly identified Crandell during prosecution as prior art disclosing the use of an "authentication token" through its disclosure of "cookies." EX1002, p. 167. In particular, the Examiner stated "Crandell further discloses intercepting at the network access controller a second request from the browser…; determining whether the second request contains an authentication token (i.e., determining whether the second request contains a cookie); and redirecting the browser application." *Id.* Applicant did not distinguish or dispute this aspect of Crandell during prosecution. Rather, Applicant instead amended the independent claims to secure allowance.

92. As **Crandell** demonstrates, it was well known in the art to use cookies

to track whether a user is authenticated and to use cookies in HTTP requests to track state information about the client device. A POSITA thus would have been motivated, and would have found it advantageous and obvious to implement **Subbiah**'s access control system using **Crandell**'s teachings of cookies in an HTTP redirect response. **Crandell**, like **Subbiah**, is in the same field and is analogous art to the '336 patent; each relates to ways of controlling access to resources across multi-domain communications networks. *E.g.*, Crandell, p.23.

93. **Crandell** is also pertinent to the alleged problem(s) identified in the '336 patent of the alleged need for controlled access to network resources. *E.g.*, EX1001, 1:34-38 ("Network access providers utilizing Access Controlled Network Sharing technology to provide user-specific provisioned access to private/public networks may also have a need to allow controlled access for unauthenticated users to a restricted collection of network destinations"); Crandell, p.23 ("Our goal was to provide a transparent firewall web proxy, a proxy allowing authorized and secure access to the many firewall-protected intranet web servers at Los Alamos National Laboratory (LANL).").

94. A POSITA would have recognized that **Crandell's** teachings of using cookies in an HTTP message would have improved **Subbiah**'s access control system and would have been an obvious implementation choice. For example, **Subbiah**'s access control system already requires the gateway to determine at step 707 whether

the network resource request is a "first time request" and will redirect the user accordingly based on a simple yes/no to that determination. Subbiah, FIG. 7. Using cookies, as taught by Crandell, would allow the server to simply look for the presence or absence of this cookie in determining whether to redirect the user to the local domain home page or to the authentication login page and, a POSITA would have found this simple process to be advantageous and easily implementable. A POSITA would have understood **Crandell**'s teachings to provide known implementation details for the redirection functionality already present in **Subbiah**.

95. In light of the foregoing, a POSITA would have found it obvious and straightforward to apply **Crandell**'s teachings in implementing **Subbiah's** system and would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality.

IX. SUMMARY OF OPINIONS

96. I have been asked to compare the references cited herein to claims 1-20 of the '336 patent (the "Challenged Claims").

a. Grounds 1 and 2: In my opinion, claims 1-18 are anticipated by, or at minimum rendered obvious over, Subbiah.

b. Ground 2: In my opinion, claims 5-8, 12-15, and 19-20 are obvious over Subbiah in view of the teachings of Hinton.

X. GROUNDS 1 AND 2 - CLAIMS 1-5-18 ARE ANTICIPATED BY, OR AT MINIMUM RENDERED OBVIOUS OVER, SUBBIAH

A. Claim 1

1. Claim 1 [pre]: "A method for automatic pre-authentication redirection of network traffic, comprising:"

97. In my opinion, Subbiah discloses or at minimum renders obvious this limitation.

98. For example, Subbiah teaches a "communications network access and control system" with a "wireless access point…configured to provide different levels of access to services[,]" including "redirect[ing] the browser of client [] to the local web server." *E.g.*, Subbiah, 13:26-14:4, 15:9-12, 17:20-24. Subbiah also teaches performing this redirection before a client is authenticated by the system. *E.g.*, *id.*, 17:16-26, FIG. 7.

99. Subbiah Figure 3 "shows a diagram of a system 300 in accordance with one embodiment of the present invention. System 300…shows components of a communications network access and control system embodiment in greater detail. As depicted in Figure 3, system 300 includes a client 340 coupled to a local network 301 via a wireless access point 330. A BURP server 320, a AAA server 321, and a local Web server 310 are coupled to the local network 301. The local network 301 is coupled to the Internet 303 via a firewall 350."

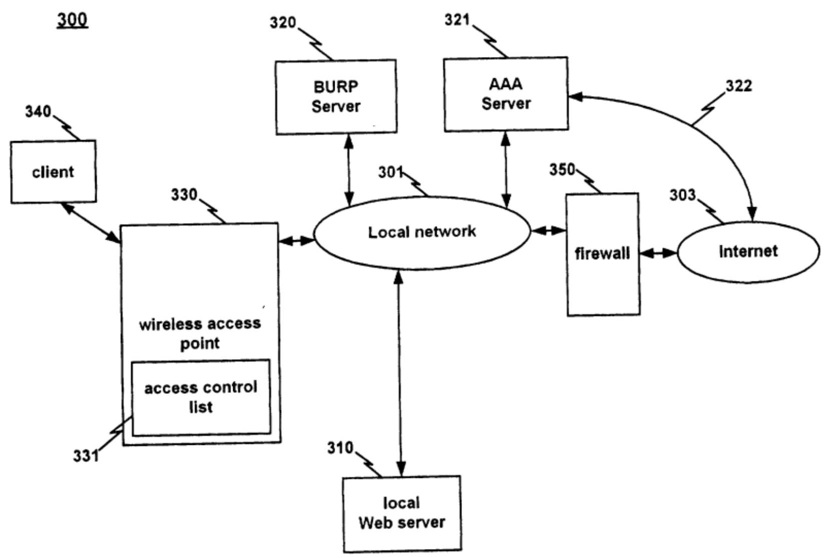
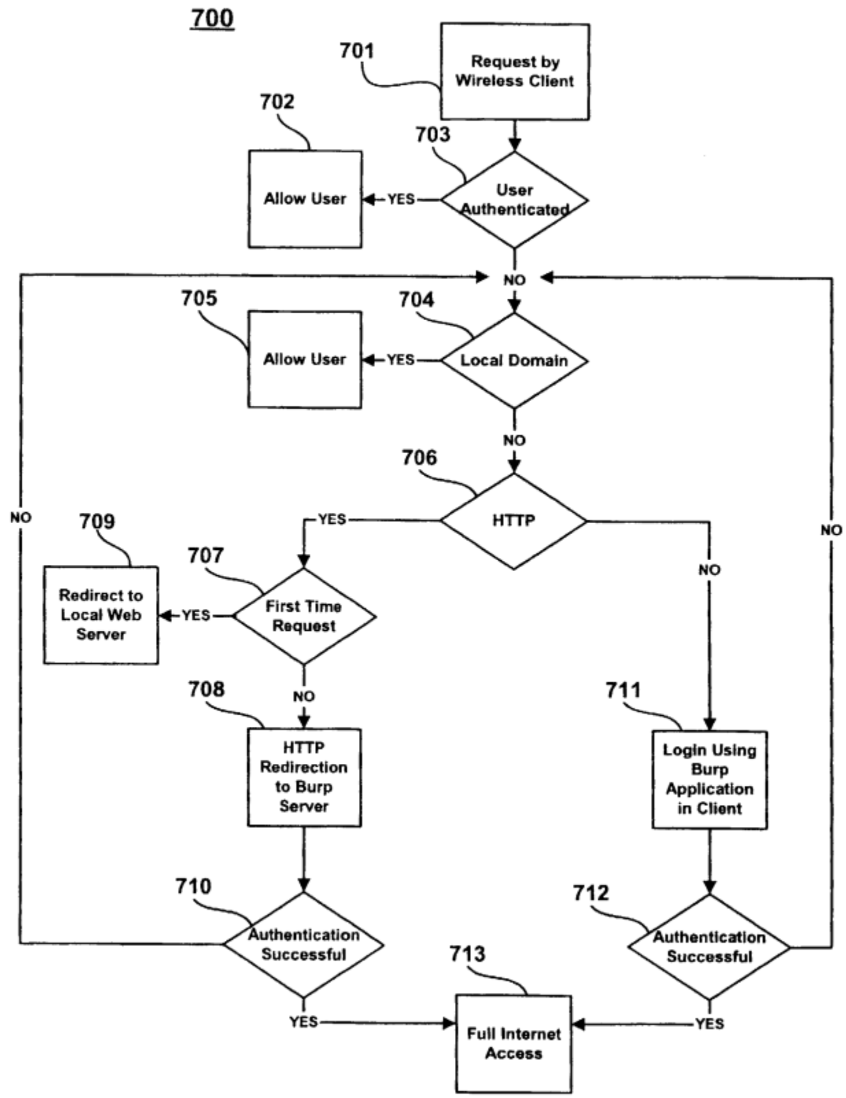


FIG. 3

100. Further, Subbiah Figure 7 "shows a flow chart of the steps of a process 700 in accordance with one embodiment of the present invention. Process 700 depicts the operating steps as performed by the components of system 300 of Figure 3." Subbiah, 17:6-8.



Subbiah, FIG. 7; *see also*, 12:7-13:17, FIG. 2

2. Claim 1[a]: "providing a network access controller in a shared network, wherein the shared network comprises a plurality of server computers and a set of network destinations hosted on the plurality of server computers;"

101. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. Subbiah discloses providing a network access controller (e.g., "wireless access point") in a shared network (e.g., "local network" or "local domain"), wherein the shared network comprises a plurality of server computers ("local web server",

"BURP Server, "AAA Server") and a set of network destinations hosted on the plurality of server computers (e.g., "free local services offered…by the local Web server", "Web pages").

102. For example, Subbiah discloses a "communications network access and control system" with a "local network" comprising multiple servers. *E.g.*, Subbiah, 13:26-14:4 ("System 300…shows components of ***a communications network access and control system*** embodiment in greater detail. As depicted in Figure 3, system 300 includes a client 340 coupled to ***a local network*** 301 via a wireless access point 330. A ***BURP server 320, a AAA server 321, and a local Web server 310 are coupled to the local network 301***."). The wireless access point—which provides network access to the client, intercepts, and redirects traffic as discussed herein, is a network access controller. *E.g.*, Subbiah, 14:2-11 ("Access to the local network 301 is provided wirelessly, via a wireless access point 330. Local content is served to the client 340 via the local Web server 310."), 15:7-12 ("[W]hen the client 340 tries to access non-local domains such as the Internet 303, ***the access point 330 will react in the following manner***. … ***the wireless access point 330 redirects the browser*** of client 340 to the local web server 310."). The local domain includes a set of network destinations hosted on the plurality of server computers, such as "Web pages provided by the local server," and pages with information about "free local services." *E.g.*, Subbiah, 5:8-10 ("[U]sers surfing the local, or internal, domain can do so freely

(e.g., ***browsing advertisements, information Web pages, event information***, and the like)…"), 10:27-11:3 ("In response to receiving a request for access to the local domain 101, access is provided to the ***services of the local domain*** 101 of the communications network. Such services include, for example, ***Web pages provided by the local server 110***."). Figures 1 and 3 further show the system, including local servers and a client on the local domain, with a wireless access point in between the client and the local domain.

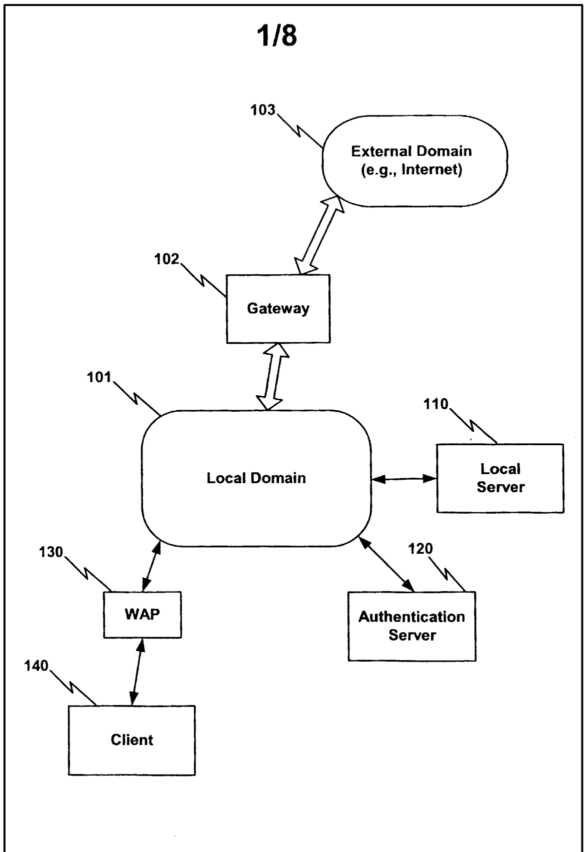


FIG. 1

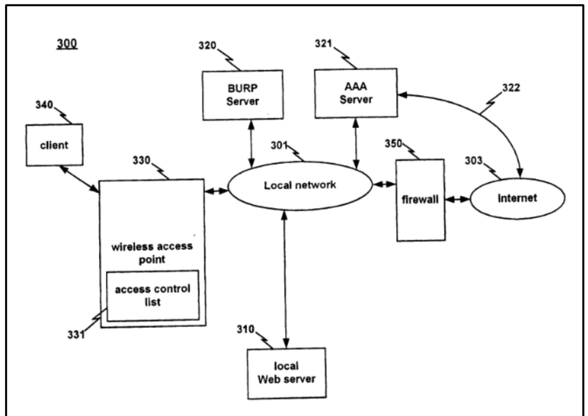


FIG. 3

3. Claim 1[b]: "intercepting at the network access controller a request to access a network resource from a browser application

running on a client device within the shared network associated with an anonymous user;"

103. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. Subbiah discloses intercepting at the network access controller ("wireless access point") a request to access a network resource from a browser application running on a client device (e.g., "PDA, laptop, cellphone", "client") within the shared network (e.g., network at "an airport terminal" or "shopping mall") associated with an anonymous user (e.g. "client", "mobile user", "Internet user[]").

104. For example, Subbiah discloses positioning the wireless access point between the client device and local domain and external domain. Subbiah, FIGs. 1, 3. In this way, the wireless access point intercepts all requests from the client device and allows or denies access accordingly. *E.g.*, Subbiah, 15:7-12 ("[W]hen the client 340 tries to access non-local domains such as the Internet 303, ***the access point 330 will react in the following manner***. If the client 340 is using a browser…the ***wireless access point 330 redirects*** the browser of client 340 to the local web server 310."), 14:27-15:1 ("***wireless access point 330 waits for a wireless client*** (e.g., client 340) ***to connect*** to the wired local network 301."), 17:10-11 ("Process 700 begins in step 701 when ***a request from the client 340 is received by the access point 330***.").

4. 1[c]: "determining whether the network resource referenced in the request is in the set of network destinations hosted on the plurality of server computers in the shared network;"

105. In my opinion, Subbiah discloses or at minimum renders obvious this

limitation. Subbiah discloses determining whether the network resource referenced in the request (*see* [1b], above) is in the set of network destinations (e.g., "Web pages") hosted on the plurality of server computers in the shared network (e.g., "local domain service", "local network").

106. For example, Subbiah discloses at step 704 of Figure 7, the wireless access point "determines whether the request form the client 340 is for a local domain service." Subbiah, 17:16-18, FIG. 7. Similarly, Subbiah teaches "a determination is made as to whether the request is for access to a first area (e.g., local domain 101) or a second area (e.g., external domain 103) of the network. As described above, the local domain of the network can include local servers (e.g., local server 110) configured to provide Web pages and information or services tailored for the characteristics of the local area (e.g., airport, shopping mall, etc.)." Subbiah, 12:20-25.

5. 1[d]: "if the network resource is in the set of network destinations hosted on the plurality of server computers in the shared network, directing the browser application running on the client device within the shared network associated with the anonymous user to the network resource; and"

107. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. Subbiah discloses determining whether the network resource referenced in the request is in the set of network destinations hosted on the plurality of server computers in the shared network (*e.g.*, "Web pages provided by the local server").

108. For example, Subbiah discloses that all "users surfing the local domain 101 can do so freely (e.g., <u>browsing</u> mall advertisements, <u>*mall informational Web pages*</u>, mall shopping event information, and the like)." Subbiah, 11:18-20. As Subbiah teaches in the flow charts of Figures 2 and 7, when the request is for a local domain, full access is freely given. *E.g.*, Subbiah, 13:12-14 ("In step 206, when the request for access to the first area is received as determined in step 202, ***access is freely provided to the information and services of the first area of the communications network***.")[11], **17:17-18** ("In step 705, if the request is for local domain 301 service, full access to the local service is provided."), FIGS 2, 7.

6. 1[e]: "if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network, redirecting the browser application running on the client device within the shared network associated with the anonymous user to a pre-authentication capture destination hosted on a first server computer, wherein the first server computer is one of the plurality of server computers in the shared network and wherein from the pre-authentication capture destination the anonymous user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network without authentication."

109. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. Subbiah discloses if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network (*e.g.*,

[11] The "first area can be ***a local domain*** of the communications network, such as, for example, ***a local Intranet of a shopping mall, airport, or the like***." Subbiah, 4:12-20.

"an Internet [] service", "external domain", "Internet"), redirecting the browser application running on the client device within the shared network associated with the anonymous user (*e.g.*, "browser" on "client") to a pre-authentication capture destination hosted on a first server computer (*e.g.*, "main, or default, Web page" residing on "local web server", "main Web page 400", "login Web page" residing on "BURP server"), wherein the first server computer is one of the plurality of server computers in the shared network (*e.g.*, on "local network", "local web server") and wherein from the pre-authentication capture destination the anonymous (*e.g.*, unauthenticated) user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network (*e.g.*, "Web pages provided by the local server") without authentication.

110. For example, the flowchart of Figure 7 illustrates how Subbiah's wireless access point redirects network traffic to a "main Web page" (also referred to as the "front page" and "splash page" of the local network) when the unauthenticated (anonymous) user attempts to access an Internet URL for the first time. Subbiah, FIG. 7. Figure 4 shows an example of this main Web page, which serves as the claimed "pre-authentication capture destination":

400

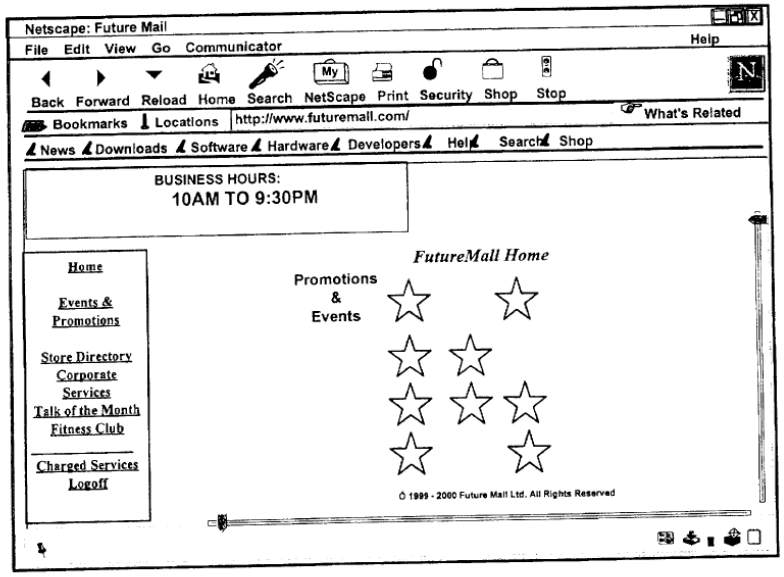


FIG. 4

Subbiah, FIG. 4. I note, for example, that the "home page" of Figure 4 also includes links to access other pages hosted on the local domain—such as the "Events & Promotions" link. *See also, e.g.*, Subbiah, 5:8-10 ("[U]sers surfing the local, or internal, domain can do so freely (e.g., browsing advertisements, information Web pages, event information, and the like)…"). In addition, at least for purposes of claim 1, Figure 5—Subbiah's "login Web page"—also acts as a "pre-authentication capture destination," as it is a pre-defined destination hosted on a server in the local domain, it is an HTML Web page, and includes a link ("HOME") from which the user can click to then browse any of the other pages hosted in the local domain. *See, e.g.*, Subbiah, FIG. 5.

111. In particular, and with reference to the flowchart of Figure 7, Subbiah

discloses an authenticated user trying to access an external (non-local) domain and redirecting that user to the local server: "In step 706, when the request is for an Internet 303 service, a determination is made as to 20 whether the client 340 is using a Web browser or not. If a Web browser is being used, process 700 proceeds to step 707. … In step 707, if the request is a first-time request, process 700 proceeds to step 709 where the request is redirected to the local web server 310. Otherwise, process 700 proceeds to step 708, where the request is redirected to the BURP server 320. In step 710, if the authentication is successful, full Internet access is provided in step 713." Subbiah, 17:18-26. And Subbiah further discloses that this redirection goes to the "home page" (as illustrated in Figure 4). Subbiah, 15:7-13 ("[W]hen the client 340 tries to access non-local domains such as the Internet 303, the access point 330 will react in the following manner. If the client 340 is using a browser and is downloading a default 10 homepage (e.g., assuming that the Web page resides somewhere in the Internet 303), ***the wireless access point 330 redirects the browser of client 340 to the local web server 310. The web server 310 then pushes the main, or default, Web page to the client's browser***, an example of which is shown in Figure 4 below."), 16:1-6 ("Figure 4 shows a diagram depicting a main, or default, Web page 400 in accordance with one embodiment of the present invention. ***The main Web page 400 is the Web page to which the browser of client 340 is redirected***. The Web page 400 typically functions as the "front page" or "splash page" of the local network 301."). Likewise, the "login Web page" of Figure 5 is another locally hosted pre-defined destination to which the user is redirected as claimed. Subbiah, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client 340 through a login Web page, an example of which is shown in Figure 5 below.").

B. Claim 2: "The method according to claim 1, wherein the network resource is at a network location external to the shared network."

112. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1]. In addition, Subbiah discloses wherein the network resource (*e.g.*, "site[]", "Web page[]") is at a network location external to the shared network (e.g., "external domain", "Internet").

113. For example, Subbiah discloses that "[i]n response to receiving ***a request for access to the external domain 103 (e.g., Web pages and/or sites on the Internet)***, and authentication process is performed on the client 140." Subbiah, 11:3-5. Similarly, Subbiah discloses—in both disclosed flowcharts—checking whether the user is accessing an external network location. Subbiah, 12:20-26 ("In step 202, a determination is made as to whether the request is for access to … a second area (e.g., external domain 103) of the network…The external domain can include the servers and other services available on the vast resources of the Internet."), 15:7-12 ("In the present embodiment, when the client 340 tries to access non-local domains

such as the Internet 303, the access point 330 will react in the following manner. If the client 340 is using a browser and is downloading a default homepage (e.g., assuming that the Web page resides somewhere in the Internet 303), the wireless access point 330 redirects the browser of client 340…"), 17:18-20 ("In step 706, when the request is for an Internet 303 service, a determination is made as to whether the client 340 is using a Web browser or not.").

C. Claim 3: "The method according to claim 1, wherein the redirecting further comprises sending from the network access controller to the client device a response containing an identifier identifying the pre-authentication capture destination."

114. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1]. Subbiah discloses wherein the redirecting further comprises sending from the network access controller to the client device a response containing an identifier identifying the pre-authentication capture destination (e.g., "http://www.futuremall.com/").

115. For example, Subbiah discloses the wireless access point determining that the user is trying to access an Internet web page (e.g., an "HTTP" request) and redirecting the user's browser to the default "home" page on the local server. Subbiah, 15:7-13 ("If the client 340 is ***using a browser*** and is downloading a default homepage (e.g., assuming that the Web page resides somewhere in the Internet 303), ***the wireless access point 330 redirects the browser of client 340 to the local web server 310***. The web server 310 then pushes the main, or default, Web page to the

client's browser, an example of which is shown in Figure 4 below."). As a POSITA would have understood, redirecting a browser to any web page necessarily requires sending from the access point to the client device an HTTP response that indicates that a redirect is indicated, and the location to which the browser should be redirected. For example, if a web site has permanently moved, the current web server will response with a "301" and a location header indicating the URL of the new location; the browser will then automatically (*i.e.,* without any action from the user) fetch the web page at the new indicated URL[12]. Indeed, Figure 4 illustrates the URL of the local domain "home page" as "http://www.futuremall.com/". Subbiah, FIG. 4.

D. Claim 4: "The method according to claim 1, further comprising: redirecting the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."

116. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1]. Subbiah discloses redirecting the browser application running on the client device back to the pre-authentication capture destination (*e.g.*, "login Web page" on "BURP server") when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality

---

[12] For a full description of redirection responses, see RFC 2616, section 10.3, "Redirection 3xx" published June 1999; see https://www.ietf.org/rfc/rfc2616.txt

of server computers in the shared network.

117. For example, Subbiah discloses providing unauthenticated users free access to the information and services of the first area—namely, the web sites hosted on the local domain servers, whenever a user attempts and fails authentication. Subbiah, 13:14-17 ("[i]n the event of an unsuccessful authentication process as determined in step 204, process 200 proceeds to step 206 and ***provides access to the information and services of the first area***."). In addition, as demonstrated in the flow charts of Fig. 7, to the extent a user attempts to access external resources, such as the Internet, after the first such attempt the process returns to step 704 and cycles through step 708 in which the user is redirected to the login Web page of Fig. 5, hosted on the BURP server, and is provided access to the pages on the local domain, including the "splash page" of the local network. Subbiah, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time, ***the access point 330 redirects the browser of client 340 to the BURP server 320***. The BURP server 320 will then try to authenticate the client 340 through a login Web page, an example of which is shown in Figure 5 below."). Again, a common behavior in 2004 (and still today) is that a failed login will send the user back to some standard or default page, often the login screen itself (or sometimes a warning screen if too many failed attempts have occurred).

E. Claim 5

1. Claim 5[pre]: "The method according to claim 1, further comprising:"

118. *See* [1].

2. Claim 5[a]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"

119. Subbiah discloses intercepting at the network access controller ("wireless access point") a second request from the browser application running on the client device associated with the anonymous (e.g., "unauthenticated") user to access a second network resource (*e.g.*, "Web page") that is not in the set of network destinations (*e.g.*, "external domain", "Internet")."

120. In addition to the disclosures discussed above with respect to [1b], Subbiah further discloses that its wireless access point can recognize multiple attempts by the same client to access external network resources. Subbiah, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time…"), FIG. 7 (step 707).

3. Claim 5[b]: "determining whether the second request contains an authentication token."

121. Subbiah discloses or at minimum renders obvious determining whether the second request contains an authentication token.

122. For example, Subbiah discloses the wireless access point intercepting a

"second" request to access a non-local resource, such as an Internet Web page and "redirect[ing] the browser" accordingly. *E.g.*, Subbiah 16:10-14. ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser…"). Subbiah expressly discloses that this is a *browser* based-attempt to access the Internet and that it is not the first such attempt. *E.g.*, *id.*, Fig. 7 (steps 706, 707, 708). A POSITA would have understood that a common way of determining whether this is an Internet browser's first or second attempt at accessing the Internet would include the use of cookies—which are unique sequences of characters—inserted into the request header, which would then be used in making redirection decisions including to the login screen on Subbiah's BURP server. The wireless access point could insert a cookie into the request header after the first attempt and each subsequent attempt would therefore include that cookie until the user is authenticated and permitted to access the Internet. At minimum, it would have been obvious to use cookies to do so in order to ensure that browsers are directed to the correct location on the local domain.

F. Claim 6: "The method according to claim 5, wherein the second request does not contain the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."

123. Subbiah discloses wherein the second request does not contain the authentication token, further comprising redirecting the browser application running

on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network.

124. For example, a POSITA would have understood that implementing Subbiah by using the presence or absence of cookies (as would have been obvious in view of Subbiah) to identify first time requests and repeat requests, would have resulted in Subbiah redirecting the client's browser back to the pre-authentication capture destination (e.g., the "home page" of the local domain) when the authentication token (e.g., cookie) is not present. *See*, e.g., elements [5a] and [5b], above; *see also, e.g.*, Subbiah, 15:7-163, 16:1-6.

G. Claim 7: "The method according to claim 5, wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."

125. *See* [5]. Subbiah discloses wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network.

126. For example, Subbiah discloses that requests subsequent to the first request—meaning, requests where the URI includes the authentication token (*see* [5a] above), the user's browser is redirected to the "login web page" of Figure 5,

hosted on the BURP server. Subbiah, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client 340 through a login Web page, an example of which is shown in Figure 5 below."), FIG. 7.

H. Claim 8: "The method according to claim 7, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network."

127. *See* [7]. Subbiah discloses wherein the anonymous user is authenticated by the second server computer for network access external to the shared network.

128. For example, Subbiah discloses the BURP server authenticating the user and permitting access to the external network. Subbiah, 16:10-14 ("[I]f the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client 340 through a login Web page, an example of which is shown in Figure 5 below."), 17:22-26 ("…the request is redirected to the BURP server 320. In step 710, if the authentication is successful, full Internet access is provided in step 713.").

I. Claim 9

1. [9pre]: "A computer program product comprising a non-transitory computer readable storage medium storing computer instructions translatable by a processor to perform:"

129. In my opinion, Subbiah discloses or at minimum renders obvious this

limitation. *See* [1.pre]. In addition, Subbiah discloses a computer program product comprising a non-transitory computer readable storage medium storing computer instructions translatable by a processor.

130. For example, Subbiah discloses that the invention is carried out by "computer system platform[s]" comprising, for example, software executed by a processor: "certain processes and steps of the present invention are realized, in one embodiment, as a series of instructions (e.g., software program) that reside within computer readable memory units of a computer system (e.g., system 812) and are executed by the processor(s) of system S12. When executed, the instructions cause the computer system 812 to implement the functionality of the present invention as described above." Subbiah, 18:6-19:4 (also describing the "basic components of an embedded computer system as implemented within a wireless access point, firewall, or gateway"), FIG. 8.

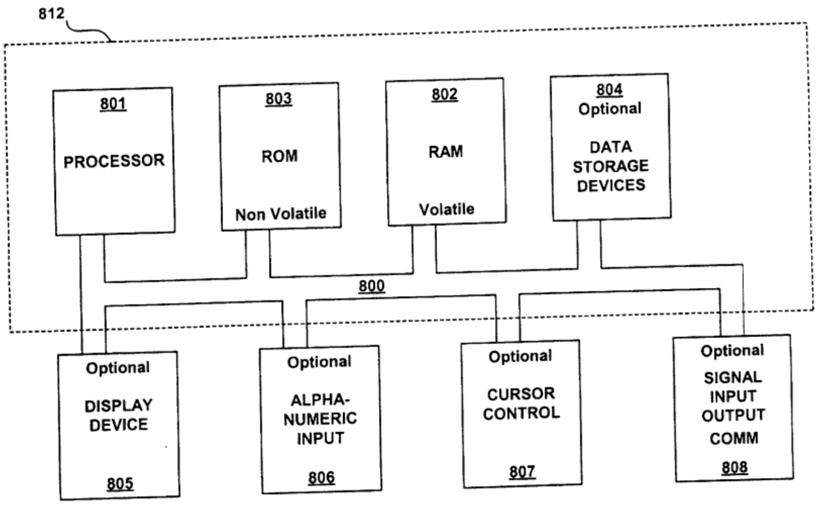


FIG. 8

2. 9[a]: "intercepting at a network access controller a request to access a network resource from a browser application running on a client device within the shared network associated with an anonymous user;"

131. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.a].

3. 9[b]: "determining whether the network resource referenced in the request is in a set of network destinations hosted on a plurality of server computers in a shared network;"

132. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.b].

4. 9[c]: "if the network resource is in the set of network destinations hosted on the plurality of server computers in the shared network, directing the browser application running on the client device within the shared network associated with the anonymous user to the network resource; and"

133. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.c].

5. 9[d]: "if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network, redirecting the browser application running on the client device within the shared network associated with the anonymous user to a pre-authentication capture destination hosted on a first server computer, wherein the first server computer is one of the plurality of server computers in the shared network and wherein from the pre-authentication capture destination the anonymous user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network without authentication."

134. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.d].

J. Claim 10: " The computer program product of claim 9, wherein the redirecting further comprises sending from the network access controller to the client device a response containing an identifier identifying the pre-authentication capture destination."

135. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [3], [9].

K. Claim 11: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform: redirecting the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."

136. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [4], [9].

L. Claim 12

1. Claim 12[a]: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform:"

137. *See* [9].

2. Claim 12[b]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"

138. *See* [9], [5a].

3. Claim 12[c]: "determining whether the second request contains an authentication token."

139. *See* [9], [5b].

M. Claim 13

1. Claim 13[a]: "The computer program product of claim 12, wherein the second request does not contain the authentication token and wherein the computer instructions are further translatable by the processor to perform:"

140. *See* [12], [6].

2. Claim 13[b]: "redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."

141. *See* [12], [6].

N. Claim 14

1. Claim 14[a]: "The computer program product of claim 12, wherein the second request contains the authentication token and

wherein the computer instructions are further translatable by the processor to perform:"

142. *See* [12], [7].

2. Claim 14[b]: "redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."

143. *See* [12], [7].

O. Claim 15

1. Claim 15[a]: "The computer program product of claim 14, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network and wherein the computer instructions are further translatable by the processor to perform:"

144. *See* [12], [8].

2. Claim 15[b]: "allowing the client device access to the second network resource."

145. *See* [12], [8].

P. Claim 16

1. 16[pre]: "An apparatus for controlling network access, comprising:"

146. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.pre], [9.pre].

2. 16[a]: "a processor within a shared network; and"

147. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. Subbiah discloses a first network interface coupled to the processor, wherein the computer instructions are further translatable by the processor to

continuously monitor for network access from client devices on the first network interface. *See* [9.pre].

3. 16[b]: "a computer readable storage medium storing computer instructions translatable by the processor to perform:"

148. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [9.pre].

4. 16[c]: "intercepting a request to access a network resource from a browser application running on a client device within the shared network coupled to the apparatus, wherein the client device is associated with an anonymous user;"

149. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.a].

5. 16[d]: "determining whether the network resource referenced in the request is in a set of network destinations hosted on a plurality of server computers coupled to the apparatus, wherein the plurality of server computers resides on the shared network;"

150. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.b].

6. 16[e]: "if the network resource is in the set of network destinations hosted on the plurality of server computers in the shared network, directing the browser application running on the client device within the shared network associated with the anonymous user to the network resource; and"

151. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.c].

7. 16[f]: "if the network resource is not in the set of network destinations hosted on the plurality of server computers in the shared network, redirecting the browser application running on the client device within the shared network associated with the anonymous user to a pre-authentication capture destination hosted on a first server computer, wherein the first server computer is one of the plurality of server computers in the shared network and wherein from the pre-authentication capture destination the anonymous user is free to visit any of the set of network destinations hosted on the plurality of server computers in the shared network without authentication."

152. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [1.d].

Q. Claim 17: "The apparatus of claim 16, wherein the computer instructions are further translatable by the processor to redirect the browser application running on the client device back to the preauthentication capture destination when the anonymous user attempts to access any network resource that is not in the set of network destinations hosted on the plurality of server computers in the shared network."

153. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [16], [4].

R. Claim 18: "The apparatus of claim 16, further comprising: a first network interface coupled to the processor, wherein the computer instructions are further translatable by the processor to continuously monitor for network access from client devices on the first network interface."

154. In my opinion, Subbiah discloses or at minimum renders obvious this limitation. *See* [16]. Subbiah discloses a first network interface coupled to the processor, wherein the computer instructions are further translatable by the processor

to continuously monitor for network access from client devices on the first network interface.

155. For example, as discussed above with reference to claims 1 and 16, Subbiah discloses that the wireless access point intercepts, reacts, and redirects traffic from the client device. *Supra*, ___. A POSITA would have understood that, to do so, the wireless access point necessarily must be continuously monitoring for communication and network requests from the client devices.

S. Claim 19

1. Claim 19: "The apparatus of claim 18, wherein the computer instructions are further translatable by the processor to perform:"

156. *See* [18].

2. Claim 19[a]: "intercepting a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"

157. *See* [18], [5a].

3. Claim 19[b]: "determining whether the second request contains an authentication token."

158. *See* [18], [5b].

T. Claim 20

1. 20[pre]: "The apparatus of claim 19, wherein the computer instructions are further translatable by the processor to perform:"

159. *See* [19].

2. Claim 20[a]: "if the second request does not contain the authentication token, redirecting the browser application running on the client device associated with the anonymous user back to the

preauthentication capture destination hosted on the first server computer in the shared network; and"

160. *See* [19], [6].

3. Claim 20[b]: "if the second request contains the authentication token, redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."

161. *See* [19], [7].

XI. GROUND 3: CLAIMS 5-8, 12-15, AND 19-20 ARE OBVIOUS OVER SUBBIAH IN VIEW OF HINTON OR CRANDELL

162. As discussed above, *Supra*, VIII.B-VIII.C, a POSITA would have been motivated and found it obvious to apply Hinton's teachings and Crandell's teachings to Subbiah's network access control system. Claims 5-8, 12-15, and 19-20 are therefore obvious over Subbiah in view of Hinton's teaching as further described below.

A. Claim 5

1. Claim 5[pre]: "The method according to claim 1, further comprising:"

163. *See* [1].

2. Claim 5[a]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"

164. *See* § X.E.2.

3. Claim 5[b]: "determining whether the second request contains an authentication token."

165. Subbiah in view of Hinton renders obvious determining whether the second request contains an authentication token.

166. To the extent it is argued that using cookies in the URL request would not have been obvious—or that a cookie is not an authentication token—Hinton discloses appending an "authentication token" to a URI when a user requests a protected resource. *See, e.g.*, Hinton, [0064] ("server…generates an introductory authentication token (step 410), ***preferably appends the token to the redirection URI, places the redirection URI in the HTTP Redirect message, and then sends the HTTP Redirect to the client*** (step 412)."). Hinton further discloses the server making determinations based on the presence or absence of that token. *E.g.*, Hinton, [0042] ("the server determines whether the client's HTTP Request contains an introductory authentication token, preferably appended to the URI (step 212). … If the HTTP message does not have an introductory authentication token, then the server forces the user at the client to complete a manual authentication process"). In other words, like the '336 patent, Hinton discloses its server determining how to react to a client request based on the presence of the authentication token.

167. Similarly, Crandell discloses using a "cookie" to determine how to direct/redirect the second request. *E.g.*, Crandell, 004 ("There are two popular methods for keeping track of authenticated web sessions:…, and one uses cookies

[6,7,8], RFC 2965 [9]."). As Crandell explains, "[t]he The cookie string is random and contains no intrinsic value or information beyond being reasonably unique and hard to guess. … The cookie is bound to the browser's IP address. … Every new HTTPS request causes the cookie to be re-verified." E.g., Crandell, 004. When the request is passed along with the appropriate cookie, the server will redirect it accordingly.

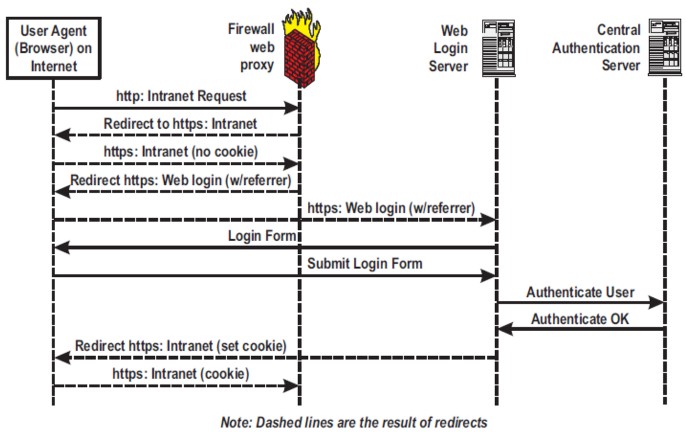


Figure 4: Initial HTTP request.

168. As discussed in §§VIII.B-VIII.C, a POSITA would have been motivated to implement Subbiah's access control system using Hinton's teachings of an authentication token in the URI or Crandell's teachings of cookies, as the basis for making redirection determinations. In particular, a POSITA would have found it obvious to use either of an authentication token (as taught by Hinton) or authentication cookie (as taught by Crandell) in step 707 of Subbiah's Figure 7, to determine if the request is a first time request requiring redirection to the Local Web Server or a repeat request requiring HTTP Redirection to Burp Server.

B. Claim 6: "The method according to claim 5, wherein the second request does not contain the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."

169. Subbiah discloses wherein the second request does not contain the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network.

170. For example, a POSITA would have understood that implementing Subbiah by using the presence or absence of cookies (as would have been obvious in view of Subbiah and/or Crandell) or an authentication token (as disclosed by Hinton) to identify first time requests and repeat requests, would have resulted in Subbiah redirecting the client's browser back to the pre-authentication capture destination (e.g., the "home page" of the local domain) when the authentication token is not present. *See*, e.g., elements [5a] and [5b], above; *see also, e.g.*, Subbiah, 15:7-163, 16:1-6.

C. Claim 7: "The method according to claim 5, wherein the second request contains the authentication token, further comprising redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."

171. *See* §X.G. This limitation is met for the same reasons as set forth in the

Grounds above; the nature of the authentication token discussed in claim 5 (*e.g.*, whether Crandell's "cookie" or Hinton's "authentication token") does not change how Subbiah reacts to the presence/absence of that token.

D. Claim 8: "The method according to claim 7, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network."

172. *See* § X.H.

E. Claim 12

1. Claim 12[a]: "The computer program product of claim 9, wherein the computer instructions are further translatable by the processor to perform:"

173. *See* [9].

2. Claim 12[b]: "intercepting at the network access controller a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"

174. *See* [9], [5a].

3. Claim 12[c]: "determining whether the second request contains an authentication token."

175. *See* [9], [5b].

F. Claim 13

1. Claim 13[a]: "The computer program product of claim 12, wherein the second request does not contain the authentication token and wherein the computer instructions are further translatable by the processor to perform:"

176. *See* [12], [6].

2. Claim 13[b]: "redirecting the browser application running on the client device associated with the anonymous user back to the pre-authentication capture destination hosted on the first server computer in the shared network."

177. *See* [12], [6].

G. Claim 14

1. Claim 14[a]: "The computer program product of claim 12, wherein the second request contains the authentication token and wherein the computer instructions are further translatable by the processor to perform:"

178. *See* [12], [7].

2. Claim 14[b]: "redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."

179. *See* [12], [7].

H. Claim 15

1. Claim 15[a]: "The computer program product of claim 14, wherein the anonymous user is authenticated by the second server computer for network access external to the shared network and wherein the computer instructions are further translatable by the processor to perform:"

180. *See* [12], [8].

2. Claim 15[b]: "allowing the client device access to the second network resource."

181. *See* [12], [8].

I. Claim 19

1. Claim 19: "The apparatus of claim 18, wherein the computer instructions are further translatable by the processor to perform:"

182. *See* [18].

2. Claim 19[a]: "intercepting a second request from the browser application running on the client device associated with the anonymous user to access a second network resource that is not in the set of network destinations; and"

183. *See* [18], [5a].

3. Claim 19[b]: "determining whether the second request contains an authentication token."

184. *See* [18], [5b].

J. Claim 20

1. 20[pre]: "The apparatus of claim 19, wherein the computer instructions are further translatable by the processor to perform:"

185. *See* [19].

2. Claim 20[a]: "if the second request does not contain the authentication token, redirecting the browser application running on the client device associated with the anonymous user back to the preauthentication capture destination hosted on the first server computer in the shared network; and"

186. *See* [19], [6].

3. Claim 20[b]: "if the second request contains the authentication token, redirecting the browser application running on the client device associated with the anonymous user to an authentication page hosted on a second server computer in the shared network."

187. *See* [19], [7].

XII. SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS

188. Neither the applicant nor the Examiner identified any secondary considerations that favored a finding of non-obviousness during prosecution of the application that issued as the '336 Patent. *See generally* EX1002. Further, I am

unaware of any secondary considerations that tend to show non-obviousness of the Challenged Claims. To the extent that such secondary considerations become available to me in the course of this proceeding, I reserve the right to address them in a supplemental declaration.

189. I declare under penalty of perjury that the foregoing is true and correct. Executed this 9th day of October, 2025 in Louisville, Colorado.

Appendix A

John R. Black, Jr.

Department of Computer Science
430 UCB
University of Colorado
Boulder, CO 80309-0430 USA

office: +1 303 492-0573
FAX: +1 303 492-2844
secretary: +1 303 492-7514

Email: jrblack@cs.colorado.edu
WWW: http://www.cs.colorado.edu/~jrblack/

Position Assoc. Prof. Computer Science, University of Colorado at Boulder *7/08–present*

Research Cryptography, Network Security, Computer Security.

Past Employment

SecureSet LLC *9/15–7/18*
Vice President of Education

University of Colorado at Boulder *7/02–7/08*
Assistant Professor of Computer Science.

University of Nevada, Reno *7/00–6/02*
Assistant Professor of Computer Science.

University of California, Davis *7/97–7/00*
Research Assistant

University of California, Davis *8/95–6/97*
Teaching Assistant

Ingres Corporation *6/88–4/94*
Senior Member of Technical Staff

Education

University of California, Davis *9/95–9/00*
Ph.D. in Computer Science.
Thesis: Message Authentication Codes.
Advisor: Phillip Rogaway.

California State University at Hayward *9/84–6/88*
B.S. in Computer Science and Mathematics, 1988.
Honors: Summa Cum Laude

Awards

NSF CAREER Award, 2002
Chancellor's Teaching Fellowship, UC Davis, 1998
Outstanding Teaching Assistant, UC Davis, 1998
Outstanding Teaching Assistant, UC Davis, 1997
A Check for $2.56 from Don Knuth, 1996

rev September 23, 2025

Journal Publications

1. P. Rogaway, M. Bellare and J. Black, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption." *ACM Transactions on Information and System Security (TISSEC)*, Volume 6, Issue 3, pp. 365–403, August, 2003.

2. J. Black, and P. Rogaway, "CBC MACs for Arbitrary Length Messages: The Three-Key Constructions." *Journal of Cryptology*, Volume 18, Number 2, pp. 111–132, Spring, 2005.

3. J. Black, "The Impossibility of Technology-Based DRM and a Modest Suggestion." *Journal of Telecommunications and High-Technology Law —JTHTL*, Volume 3, Number 2, pp. 387–396, Spring, 2005.

4. J. Black, M. Cochran and R. Gardner, "An Analysis of the Internet Chess Club." *IEEE Security and Privacy*, Volume 4, Number 1, pp. 46–52, January, 2006.

5. J. Black, M. Cochran and T. Shrimpton, "On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions." *Journal of Cryptology*, Volume 22, Number 3, pp. 311–329, Fall, 2009.

6. J. Black, P. Rogaway, T. Shrimpton, and M. Stam "An Analysis of the Blockcipher-Based Hash Functions from PGV." *Journal of Cryptology*, Volume 23, Number 4, pp. 519–545, Fall, 2010.

7. C. Wilks, M. Cline, E. Weiler, M. Diehkans, B. Craft, C. Martin, D. Murphy, H. Pierce, J. Black, D. Nelson, B. Litzinger, T. Hatton, L. Maltbie, M. Ainsworth, P. Allen, L. Rosewood, E. Mitchell, B. Smith, J. Warner, J. Groboske, H. Telc, D. Wilson, B. Sanford, H. Schmidt, D. Haussler, D. Maltbie "The Cancer Genomics Hub (CGHub): overcoming cancer through the power of torrential data." *Database*, Volume 2014, doi: 10.1093/database/bau093.

Book Chapters

1. J. Black, "Cryptography." Invited article for the Encyclopedia of Life Support Systems under the auspices of UNESCO. See `http://www.eolss.net`. 14 pages, March, 2004.

2. J. Black, "Authenticated Encryption." Invited article for the *Encyclopedia of Cryptography and Security*, Springer-Verlag. 12 pages. August, 2005.

Conference Publications (Refereed)

1. J. Black, C. Martel, and H. Qi, "Graph and Hashing Algorithms for Modern Architectures: Design and Performance." *Workshop on Algorithm Engineering — WAE '98*, Saarbrücken, Germany. Second Workshop on Algorithm Engineering, proceedings, pp. 37–48. Full version of this paper available at `theory.cs.ucdavis.edu`.

2. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and Secure Message Authentication." *Advances in Cryptology — CRYPTO '99*, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 216–233, 1999. Full version and updated version of this paper available at `www.cs.ucdavis.edu/~rogaway/umac`.

3. J. Black and P. Rogaway, "CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions." *Advances in Cryptology — CRYPTO 2000*, Lecture Notes in Computer Science, Vol. 1880, Springer-Verlag, pp. 197–215, 2000.

4. P. Rogaway, M. Bellare, J. Black and T. Krovetz, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption." *Eighth ACM Conference on Computer and Communications Security (CCS-8)*, ACM Press, pp. 196–205, 2001.

5. J. Black and P. Rogaway, "Enciphering Finite Sets of Arbitrary Size." *RSA Data Security Conference, Cryptographer's Track (RSA-CT)*, Lecture Notes in Computer Science, Vol. 2271, Springer-Verlag, pp. 114–130, 2002.

6. J. Black and P. Rogaway, "A Block-Cipher Mode of Operation for Parallelizable Message Authentication." *Advances in Cryptology — EUROCRYPT 2002*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 384–397, 2002.

7. J. Black and H. Urtubia, "Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption." *USENIX Security Symposium — Security '02*. 10 pages, 2002.

8. J. Black, P. Rogaway, and T. Shrimpton, "Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV." *Advances in Cryptology — CRYPTO 2002*, Lecture Notes in Computer Science, Vol. 2442. 16 pages, 2002.

9. J. Black, P. Rogaway, and T. Shrimpton, "Encryption Scheme Security in the Presence of Key-Dependent Messages." *Selected Areas in Cryptography — SAC 2002*, Lecture Notes in Computer Science, Vol. 2595, 14 pages, 2002.

10. R. Motwani, J. Breidenbach and J. Black, "Collocated Dataglyphs for Large Message Storage and Retrieval." *Security, Steganography, and Watermarking of Multimedia Contents VI*, Society for Imaging Science and Technology (I&ST) jointly with International Society for Optical Engineering (SPIE), Vol. 5306, 19 pages, 2004.

11. J. Black, M. Cochran and T. Shrimpton, "On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions." *Advances in Cryptology — EUROCRYPT 2005*, Lecture Notes in Computer Science, Vol. 3494, Springer-Verlag, pp. 526–541, 2005.

12. J. Black, M. Cochran and R. Gardner, "Lessons Learned: A Security Analysis of the Internet Chess Club.", *Annual Computer Security Applications Conference — ACSAC 2005*, Tucson AZ, USA, pp. 220–228, 2005.

13. J. Black and M. Cochran and T. Highland, "A Study of the MD5 Attacks: Insights and Improvements", *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 262–277, 2006.

Conference Publications (cont.)

14. J. Black, "The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function.", *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 328–340, 2006.

15. J. Black, "Compare-by-Hash: A Reasoned Analysis", *USENIX Annual Technical Conference — USENIX 2006*, 8 pages, 2006.

16. J. Black and M. Cochran, "MAC Reforgeability", *Fast Software Encryption — FSE 2009*, Lecture Notes in Computer Science, Vol. 5665, Springer-Verlag, pp. 345–362, 2009.

17. J.H. Huang, J. Black, and S. Mishra, "Security and Privacy in a Sensor-Based Search and Rescue System," *1st ICST/CREATE-NET International Conference on Ad Hoc Networks — ADHOCNETS 2009*, Vol. 28, Springer.

18. A. Sayler, D. Grunwald, J. Black, E. White, M. Monaco, "Supporting CS education via virtualization and packages: tools for successfully accommodating "bring-your-own-device" at scale," *SIGCSE 2014*, pp. 313-318, 2014.

Workshop Publications (Non-Refereed)

1. J. Black and P. Rogaway, "A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC." *NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000*, 4 pages, Sep 2000.

2. J. Black and P. Rogaway, "OCB: Proposal to NIST." *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 36 pages, Aug 2001.

3. J. Black and P. Rogaway, "PMAC: Proposal to NIST." *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 27 pages, Aug 2001.

Selected Talks

1. Data Structures for Fast Graph Algorithms. Presented at the 1997 UC Davis Workshop on Computing, Davis, USA, October 1997. (See Conference Publication #1.)

2. UMAC: Fast and Secure Message Authentication. Presented at CRYPTO '99, Santa Barbara, USA, August 1999. (See Conference Publication #2)

3. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Presented at CRYPTO 2000, Santa Barbara, USA, August 2000. (See Conference Publication #3)

4. A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC. Presented at NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000, October, 2000; also presented at the 2nd NIST Modes Workshop in Santa Barbara, USA, August 2001.

5. Enciphering Finite Sets of Arbitrary Size. Presented at RSA-CT '02, San Jose, USA, February 2002. (See Conference Publication #5)

6. A Block-Cipher Mode of Operation for Parallelizable Message Authentication. Presented at EUROCRYPT 2002, Amsterdam, The Netherlands, May 2002. (See Conference Publication #6)

7. Side-Channel Attacks on Symmetric Encryption Schemes. Presented at USENIX Security 2002, San Francisco, USA, August 2002. (See Conference Publication #7)

8. Practical Cryptography and Autonomic Web Computing. Invited talk at the 47th meeting of the IFIP Working Group 10.4. Rincon, Puerto Rico, January 2005.

9. On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. Presented at EUROCRYPT 2005, Aarhus, Denmark, May 2005. (See Conference Publication #11)

10. The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function. Presented at FSE 2006, Graz, Austria, March 2006. (See Conference Publication #14)

11. Compare-by-Hash: A Reasoned Analysis. Presented at USENIX Technical Conference 2007, Boston, MA, June 2006. (See Conference Publication #15)

Patents

1. T. McSheery, J. Black, S. Nollet, J. Johnson, and V. Jivan. Distributed-Processing Motion Tracking System for Tracking Individually Modulated Light Points. US Patent 6,324,296 B1. November 2001.

Funding

1. NCIIA E-Team Grant. "Entrepreneurship for Undergraduates." PI: John Black. Period: 2000-2001. Amount: $6,000.

2. University of Nevada Junior Faculty Research Grant. "Fast, Provably-Secure Cryptography." PI: John Black. Period: 2001-2002. Amount: $10,000.

3. NSF CAREER Award. "Highly-Optimized Provably-Secure Cryptography." PI: John Black. Period: 2002-2007. Amount: $469,925.

4. NSF NeTS Grant. "NeTS ProWIN: Topology And Routing With Steerable Antennas." PI: Dirk Grunwald. Co-PIs: John Black, Douglas Sicker. Period: 2005–2008. Amount: $745,215.

5. NSF Cybertrust Grant. "Cryptography for Constrained Environments." PI: John Black. Period: 2005–2008. Amount: $294,887.

Teaching History

ECS 122A — Design and Analysis of Algorithms (UC Davis). Co-taught once with Professor Rogaway; subsequently taught the course independently.
CMPSC 290G — Intro to Cryptoanalysis (UCSB).
CS 365 — Discrete Mathematics (UNR).
CS 425 — Software Engineering (UNR).
CS 426 — Senior Projects (UNR). Supervised 11 group projects in topics ranging from fingerprint recognition to audio editing to GUI design.
CS 432 — Computer Networks (UNR). Introduction to low-level networking concepts with an emphasis on network security.
CS 665 — Graduate Analysis of Algorithms (UNR). A typical algorithms course with emphasis on complexity theory.
CS 709 — Modern Cryptography (UNR). A graduate course introducing cryptography and visiting some of the research front.
CS 791G — Computer Network Security (UNR). A seminar course covering various topics related to network security.
CSCI 2270 — Data Structures (CU); Program design, Object orientation, Java, Linked lists, Arrays, Stacks and Queues, Hash tables, Trees, Balanced Binary Trees, Multi-core programming.
CSCI 3104 — Algorithms (CU); Divide-and-conquer, Greedy, Graph Algorithms, NP-Completeness, Quantum Algorithms.
CSCI 3753 — Operating Systems (CU); Scheduling, Virtual Memory, Filesystems, Multi-core systems, Pthreads, Kernel data structures, virtualization, Security.
CSCI 4830 — Network Security (CU); a new course developed to introduce basics of cryptography and network security. Covers SSL, PKI, DDOS attacks, wireless security, buffer overruns, and more.
CSCI 4900 — Solving Puzzles with Computers (CU); a one-unit undergraduate course describing some hard combinatorial puzzles and how computers can be used to attack them.
CSCI 5413 — Ethical Hacking (CU): Network security, nmap, netcat, Kali Linux, Buffer overruns, Format string vulnerabilities, Race Conditions, Web Security, SQL Injections, XSS, CSRF, Wireless.
CSCI 6268 — Foundations of Computer and Network Security (CU); an introductory course covering basic cryptography, cryptographic protocols, attacks, and principles, as well as core network security attack and defense.
CSCI 7000 — Cryptography Seminar (CU); A graduate course introducing basic cryptographic definitions and then making some forays to the research front.
CSCI 7000 — Cryptanalysis Seminar (CU); A graduate course introducing students to cryptanalysis. Differential and linear cryptanalysis, square attack, RSA basics, factoring, protocol errors, lattices, Coppersmith's algorithm.
CSCI 7000 — Quantum Computing (CU): Introduction to quantum circuits, number theory, Shor's Algorithm, Grover's Algorithm.

Graduate Students

Rakhi Motwani, M.S., Completed: Spring 2002.
Scott Fritzinger, M.S., Completed: Summer 2002.
Hector Urtubia, M.S., Completed: Spring 2003.
Hiba Fayoumi, M.S., Completed: Summer 2004.
Mary Hedges, M.S., Completed: Spring 2007.
Joesph Dunn, Ph.D., co-advisor with John Bennett, Completed: Summer 2007.
Martin Cochran, Ph.D., Completed: Spring 2008.
Jared Nishikawa, Ph.D., Completed: Spring 2016.

Undergraduate Students	Troy Trimble, University of California at San Diego. REU Student, Summer 2003. Gagan Sekhon, California State University at Hayward. REU Student, Summer 2003. Ryan Gardner, University of Colorado at Boulder. REU Student, Summer 2004. Trevor Highland, University of Texas at Austin. REU Student, Summer 2005.

External Service

Secretary, International Association for Cryptologic Research, 2005–2007.
Program Committee, ACNS 2015.
Program Committee, CT-RSA 2015.
Program Committee, FSE 2014.
Program Committee, CT-RSA 2014.
Program Committee, CT-RSA 2013.
Program Committee, Eurocrypt 2012.
Program Committee, FSE 2011.
Program Committee, PKC 2011.
Program Committee, CANS 2010.
General Chair, CRYPTO 2009.
Program Committee, CRYPTO 2008.
Program Committee, ACNS 2008.
Program Committee, RSA-CT 2007.
Program Committee, ISC 2007.
Program Committee, ACNS 2007.
Program Committee, ACM CCS 2006.
Program Committee, CANS 2006.
Program Committee, ICISC 2006.
Program Committee, SECRYPT 2006.
Program Committee, ACSAC 2006.
Program Committee, CRYPTO 2005.
Program Committee, SAC 2005.
Program Committee, ICISC 2005.
Program Committee, CANS 2005.
Program Committee, IEEE SISW 2005.
Program Committee, CRYPTO 2004.
Program Committee, EUROCRYPT 2004.
Program Committee, RSA-CT 2003.
NSF CISE Panelist, 2001, 2003, 2005, 2006, 2007, 2009.
Referee for Journal of Cryptography, 1999-2006.
Referee for Software: Practice and Experience, 2005.
Referee for IEEE Communications Magazine, 2005.
Referee for IEEE Transactions on Circuits and Systems I, 2005.
Referee for IEEE Computer, 2005.
Referee for Journal of Computer Security, 2004.
Referee for IEEE Transactions on Information Theory, 2003.
Referee for IEEE Transactions on Computers, 2002.
Reviewer for CRYPTO 1999–2002, SODA 1998, SPAA 2002, Asiacrypt 2004, EUROCRYPT 2006.

Developed `CryptoStats` web site: an application which tracks publication rates by year, by author, by conference in the two main cryptography conferences. It was heavily used in my community (on average 240 hits per month), 2003-2009.

ACM Programming Contest problem composer, 2003–2007.
ACM Programming Contest site administrator, 2005.

Graduate Student Mixer organizer, CRYPTO 2005.

Internal Service

Chair, Computing Committee, 2010–2011, 2012–2015.
Chair, Space Committee, 2012–2015.
Liaison, Casey Feldman Foundation, 2010–2015.
Member, Departmental Executive Committee, 2003–2005, 2007–2009, 2013-2015.
Member, Executive Committee, Computer and Communications Security Center, 2003–2006.
Member, Departmental Search Committee, 2003–2006, 2012–2014.
Chair, Departmental Search Committee, 2008–2009.
Member, Graduate Committee, 2005–2006.
Developed departmental voting software, now used for all departmental votes and college votes.