

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET, INC.,
Petitioner,

v.

LIONRA TECHNOLOGIES LTD.,
Patent Owner.

U.S. Patent 7,302,708
Issue Date: November 27, 2007

Title: ENFORCING COMPUTER SECURITY UTILIZING AN ADAPTIVE
LATTICE MECHANISM

Inter Partes Review No.: IPR2024-00176

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 7,302,708
UNDER 35 U.S.C. §§ 311-319 and 37 C.F.R. §§42.1-.80, 42.100-.107**

Mail Stop “PATENT BOARD”

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

Petitioner’s Exhibit List iv

I. INTRODUCTION 1

II. OVERVIEW 1

III. GROUNDS FOR STANDING.....2

IV. REASONS FOR THE REQUESTED RELIEF 2

 A. Summary of the ’708 Patent.....2

 B. Prosecution History 11

 C. Claim Construction.....13

 D. Priority of the Challenged Claims 28

 E. Person of Ordinary Skill in the Art 28

 F. State of the Art 29

 1. Well-known sensitivity-based (i.e., “access levels”) access control methods.....29

 2. Well-known method of organizing data: aggregation of nodes in a tree hierarchy.....35

 3. Well-known use of patterns of behavior/temporal access patterns in computer security and access control 36

V. IDENTIFICATION OF CHALLENGES 38

 A. Challenged Claims 38

 B. Statutory Grounds for Challenges 38

 C. Prior Art Basis 38

VI.	IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	39
A.	Ground 1: Claims 10-14 Are Obvious Over Gladstone (EX-1004) and Salazar (EX-1009).....	39
1.	Gladstone	39
2.	Salazar	43
3.	Motivation to combine Gladstone and Salazar	49
4.	Detailed Application to the Challenged Claims	50
VII.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION	86
A.	The Board Should Not Deny Institution Under 35 U.S.C. § 325(d)	86
B.	The Board Should Not Deny Institution Under 35 U.S.C. § 314(a).....	87
VIII.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	90
A.	Real Party-in-Interest (37 C.F.R. §42.8(b)(1)).....	90
B.	Related Matters (37 C.F.R. §42.8(b)(2)).....	90
1.	Judicial Matters	90
2.	Administrative Matters	90
C.	Lead/Back-up Counsel (37 C.F.R. §42.8(b)(3))	91
D.	Notice of Service Information (37 C.F.R. §42.8(b)(4))	92
IX.	CONCLUSION.....	92

Petitioner's Exhibit List

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent 7,302,708 (“the ’708 Patent”)
1002	Prosecution history of the ’708 Patent (“File History”)
1003	Declaration of Dr. Paul C. Clark (“Clark” or “Expert”)
1004	U.S. Patent No. 7,290,266 to Gladstone et. al. (“Gladstone”)
1005	U.S. Patent Application Publication No. 2005/0076030 to Hada et. al. (“Hada”)
1006	(Reserved)
1007	U.S. Patent No. 6,453,418 to Ooki et al. (“Ooki”)
1008	U.S. Patent No. 6,446,077 to Straube et al. (“Straube”)
1009	U.S. Patent Application Publication No. 2004/0122792 to Salazar (“Salazar”)
1010	U.S. Patent No. 6,334,121 to Primeaux et al. (“Primeaux”)
1011	Lane et al., <i>Sequence Matching and Learning in Anomaly Detection for Computer Security</i> , AAI Technical Report WS-97-07 (1997)
1012	U.S. Patent Application Publication No. 2005/0038881 to Ben-Itzhak (“Ben-Itzhak”)
1013	Department of Defense Standard, DoD 5200.28-STD, <i>Department of Defense Trusted Computer System Evaluation Criteria</i> (1983)
1014	U.S. Patent Application Publication No. 2002/0147924A1 to Flyntz (“Flyntz”)
1015	(Reserved)
1016	Dorothy et al., <i>Cryptography and Data Security</i> (Purdue University 1982)
1017	Infringement Contentions, <i>Lionra Techs. Ltd. v. Cisco Sys., Inc.</i> , E.D. Tex. Case No. 2:22-cv-00305-JRG-RSP (served Nov. 3, 2022)
1018	Docket Control Order, <i>Lionra Techs. Ltd. v. Cisco Sys., Inc.</i> , E.D. Tex. Case No. 2:22-cv-00305-JRG-RSP, Dkt. 55-1 (Dec. 1, 2022)
1019	U.S. District Courts – Federal Court Management Statistics – Comparison Within Circuit – During the 12-Month Period Ending September 30, 2022, available at https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distpr ofile0930.2022.pdf

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311 *et seq.* and 37 C.F.R. §§ 42.1 *et seq.*, Fortinet, Inc. (“Petitioner”) hereby petitions for *inter partes* review of U.S. Patent No. 7,302,708 (“’708 Patent”) (Ex-1001). Petitioner respectfully submits that Claims 10-14 (the “Challenged Claims”) of the ’708 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art references discussed herein. This Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of these claims. Accordingly, it is respectfully requested that the Board institute *inter partes* review of the ’708 Patent pursuant to 37 C.F.R. § 42.108.

II. OVERVIEW

The Challenged Claims are unpatentable as obvious over the prior art. The claims are directed to prior art systems and combinations of conventional components that perform a conventional function of identifying/using patterns of behavior including, “temporal access patterns,” in determining whether to grant access requests to a computer system, which was well known in computer and information security before the priority date of the ’708 Patent. The ’708 Patent admits that the prior art employed “usage patterns” in computer security, but faults the art, incorrectly, for merely “flagging suspicious activity” and not “enforc[ing]”

“a security policy based on such flagging.” EX-1001 1:46-51; §IV.F.3; EX-1003 ¶30.

III. GROUNDS FOR STANDING

Petitioner certifies that the '708 Patent is available for *inter partes* review and Petitioner is not barred or estopped from requesting this review. 37 C.F.R. § 42.104(a). This Petition is filed under 37 C.F.R. § 42.106(a).

IV. REASONS FOR THE REQUESTED RELIEF

As explained in §§ II and V-VI of this Petition and in the attached Declaration of Petitioner's Expert, Dr. Paul C. Clark. (“Clark”) (EX-1003), the systems and methods of using patterns of behavior, including “temporal access patterns” for computer and information security, as described and claimed in the '708 Patent, were obvious over the prior art to a person of ordinary skill in the art (“POSA”) at the time of the invention.

A. Summary of the '708 Patent

The '708 Patent is directed to methods and systems for ensuring secure access to computer systems. EX-1001 1:7-11, 1:55-56, 10:16-17, 11:15-16, 11:34. It describes controlling access to various “nodes” of a computer system organized in the form of a “**tree hierarchy**” as shown in Figure 1:



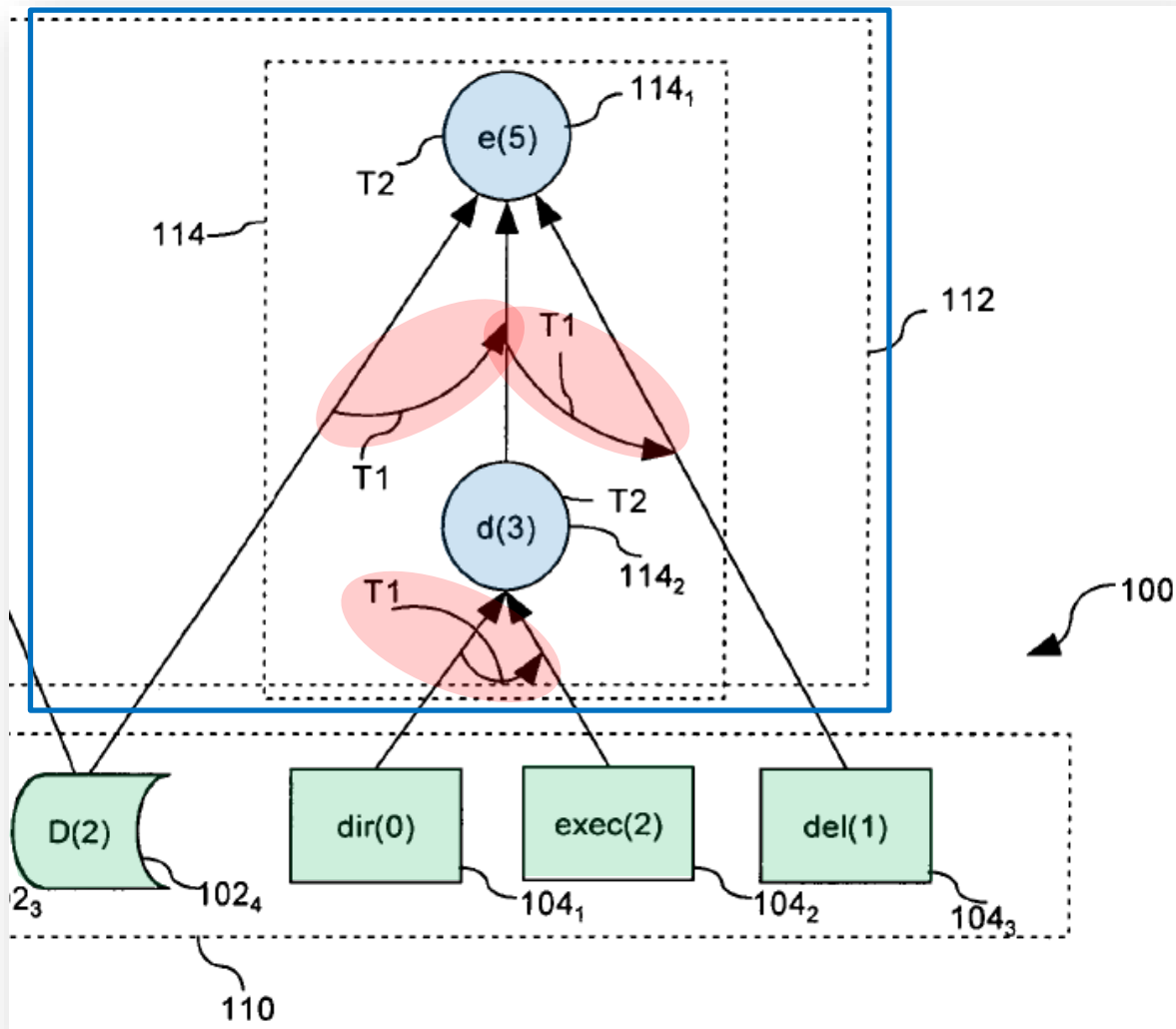
EX-1001 1:59-62, 2:67-3:6, 10:18-21, FIG. 1 (annotated).¹ Figure 1 illustrates two types of nodes: **base (or leaf) nodes 110** and **higher level (or aggregation) nodes 112**. EX-1001 3:44-49. **Base nodes 110** can be formed from “security access primitives” and can represent, or define, “various object types” 102₁-102₄ (*e.g.*, types of information), as well as system functions 104₁-104₃ (*e.g.*, directory (dir), execute (exec), and delete (del) functions). EX-1001 2:67-3:6, 3:10-47. Each node 110 can have a minimum required security access level that is indicated using a

¹ Emphasis, including coloring, made in this Petition is added unless stated otherwise.

parenthetical. In Figure 1, the number “2” in node “**D(2)**” indicates that “information type D” has a minimum required security access level of two. *Id.* If an “access authorization level” or “security access level” of a user making the request to the node is less than the minimum required security access level specified for that node, the request is rejected. EX-1001 1:59-62, 6:4-10.² EX-1003 ¶31.

Figure 1 also shows “**higher-level**” or “**aggregation**” nodes **112** that “represent information aggregation sets and/or **temporal patterns of access**” of **base nodes 110** (or other **higher-level nodes**), *e.g.*:

² As demonstrated in §§ IV.B and IV.F.1, this subject matter was well known, even according to the ’708 Patent.

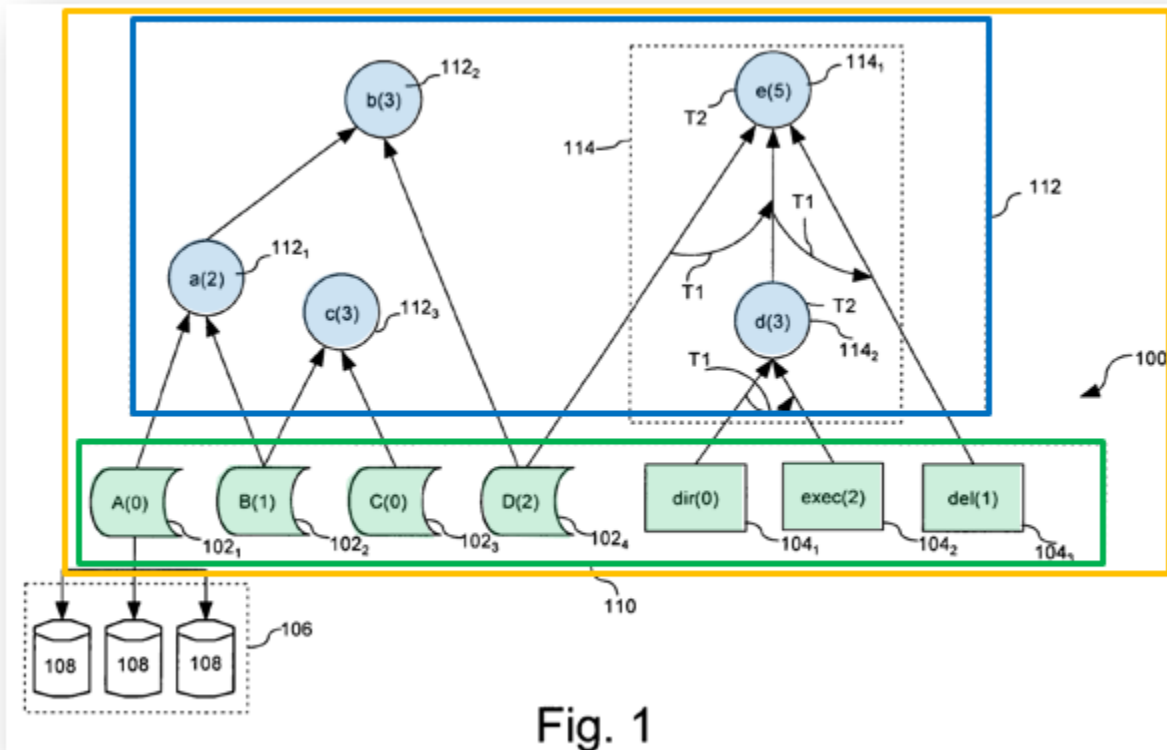


EX-1001 3:2-6, FIG. 1 (annotated). **Aggregation nodes 112** are comprised of two or more of **base nodes 110**, other **aggregation nodes 112**, or some combination of both. EX-1001 6:13-16. The '708 Patent states that “**aggregation nodes** will often have a higher minimum required security level” compared to **base nodes 110** “because aggregated data is often of a more sensitive nature.” EX-1001 6:16-23. The '708 Patent acknowledges that “[c]onsequently **aggregated information** will inevitably be of greater interest to unauthorized users and system administrators

will naturally wish to impose higher level restrictions on its access.” EX-1001

6:23-26. EX-1003 ¶32.

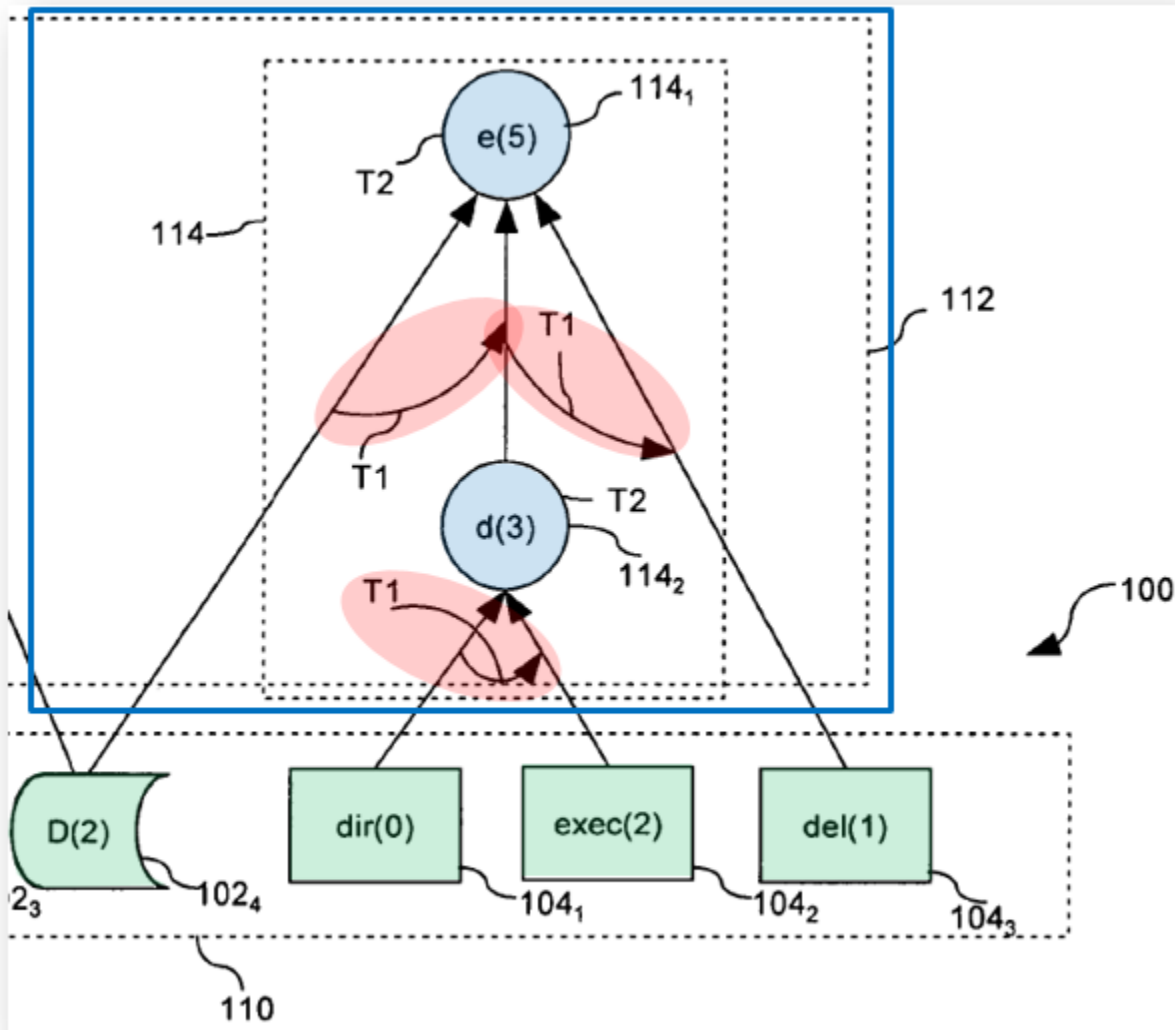
The '708 Patent describes that **aggregation nodes 112** and **base nodes 110** are logically organized into “**hierarchical tree 100**”:



EX-1001 3:44-49, FIG. 1 (annotated); EX-1003 ¶33.

Aggregation nodes 112 can represent “**temporal patterns of access**” that can be used to determine whether a user’s access request completes a temporal access pattern as part of its access control method. EX-1001 1:62-64, 4:12-16. A temporal access pattern “denote[s] a **temporal ordering**” by which the nodes are

accessed. EX-1001 4:3-15, FIG. 1. For example, **higher-level node “d(3)” 114₂** defines temporal ordering **T1** of the functions **104₁** and **104₂**:



Id. For the security policy associated with node **d(3) 114₂** to be activated, not only must both **104₁** and **104₂** be accessed but they must be accessed in the order indicated—*i.e.*, **104₁ before 104₂ (104₁ → 104₂)**. *Id.*; EX-1003 ¶34.

In addition to Figure 1’s illustration of a temporal access pattern, the ’708 Patent also describes determining whether the **order (temporal access pattern)**

required is met by comparing the time stamps in a Temporal Access Table, an example of which is provided in Figure 4B, to a Temporal Order Table, an example of which is provided in Figure 3:

Temporal Order Table (TOT)							
TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

EX-1001 FIG. 3. This Temporal Order Table captures the relative temporal order of actions and allows relative or approximate temporal pattern matching. EX-1001 4:30-33; EX-1003 ¶35.

Temporal Access Table (TAT)							
Usr	A	B	C	D	dir	exec	del
1(1)					102	112	
2(1)							
3(2)					111	103	
4(1)							
5(3)							

EX-1001 FIG. 4B. This Temporal Access Table maintains a history of what operations are performed by a user and when those operations are performed. EX-1001 5:55-57. The order of the performance of these operations may be compared to a defined **temporal access pattern**. EX-1001 5:59-61. As shown in Figure 4B, user 1 performs a **“dir” operation 104₁** at time 102 and then requests an **“exec” operation 104₂** at time 112. Since time 112 is after time 102, this request matches the **temporal access pattern** illustrated for **node “d” 114₂** of Figure 1 and, hence, the security policy associated with **node “d” 114₂** would be evaluated. EX-1001 5:62-66, FIG. 1. In this example, this request would be denied because user 1’s access level of “1” (*see* parenthetical following user 1 in Figure 4B, above) is less than the minimum access level required by node d—level “3.” *Id.* 5:62-66, FIGs. 1, 4B; EX-1003 ¶35.

The '708 Patent issued with 17 claims. Claims 1 and 9 are independent method claims and Claim 10 is an independent system claim. Claim 10 is representative:

[10pre] A secure computer system comprising:

[10a] a plurality of logical base nodes representing at least one of an
information type and a computer system function;

[10b] a plurality of higher-level nodes arranged together with said base nodes
in the form of a tree hierarchy;

[10c] a computer system interface capable of receiving a request from an
entity with a predetermined access level for access to a first base node;

[10d] a temporal access table;

[10e] processing means programmed for comparing said access request to said
temporal access table to determine if said access request completes a
prohibited temporal access pattern for said entity, and for comparing a
minimum access level established for said first base node to said
predetermined access level; and

[10f] wherein said processing means denies said request if said access request
completes a prohibited temporal access pattern for said entity and
grants said access request only if it does not complete a prohibited

temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

However, controlling access to computer systems based on the temporal access pattern based on the order of a user's requests was well known in the art and commonly used long before the '708 Patent as demonstrated by this Petition and the Declaration of Dr. Clark. EX-1003 ¶37.

B. Prosecution History

The '708 Patent issued from U.S. 10/798,074, filed on March 11, 2004. Ex-1001 (21, 22, 45); Prosecution history of the '708 Patent ("File History") (Ex-1002). The Examiner subjected U.S. 10/798,074 to a single office action, rejecting the claims under 35 U.S.C. §§101 and 103 over U.S. 2004/0044655 to Cotner ("Cotner"). EX-1002 129-140.

The Applicant addressed the §101 rejection by adding the following limitations:

- Limitations [1e] and [9e]: "denying said request if said access request completes a prohibited temporal access pattern for said entity."
- Limitation [10f]: "wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and"

EX-1002 115-119, 120.³ The Applicant argued against the §103 rejection, stating that Cotner disclosed only “controlling access to a relational database based solely on security levels”—or “access levels.” EX-1002 123; EX-1003 ¶39. The Applicant stated Cotner’s “security levels” did not disclose:

- “determining if an access request completes a **prohibited temporal access pattern** for an entity,”
- “granting the access request only if it does not complete a **prohibited temporal access pattern** for the entity,” or
- “a secure computer system comprising a processing means programmed for comparing an access request to the temporal access table to determine if the access request completes a **prohibited temporal access pattern** for an entity.”

Ex-1002 122-124. The ’708 Patent subsequently issued without further substantive comments from the Examiner. EX-1002 003-016.

However, as demonstrated by this Petition and the Declaration of Dr. Clark, determining temporal access patterns and enforcing security policies based on

³ Original Claims 1, 10, and 11, to which these amendments were made, issued as Claims 1, 9, and 10, respectively. EX-1002 019.

those patterns was well understood and widely implemented prior to the subject matter claimed in the '708 Patent. EX-1003 ¶40.

C. Claim Construction

The claims should be given “their ordinary and customary meaning” as understood by a person of ordinary skill at the time of the claimed invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312, 1327 (Fed. Cir. 2005). Petitioner proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction. EX-1003 ¶41.

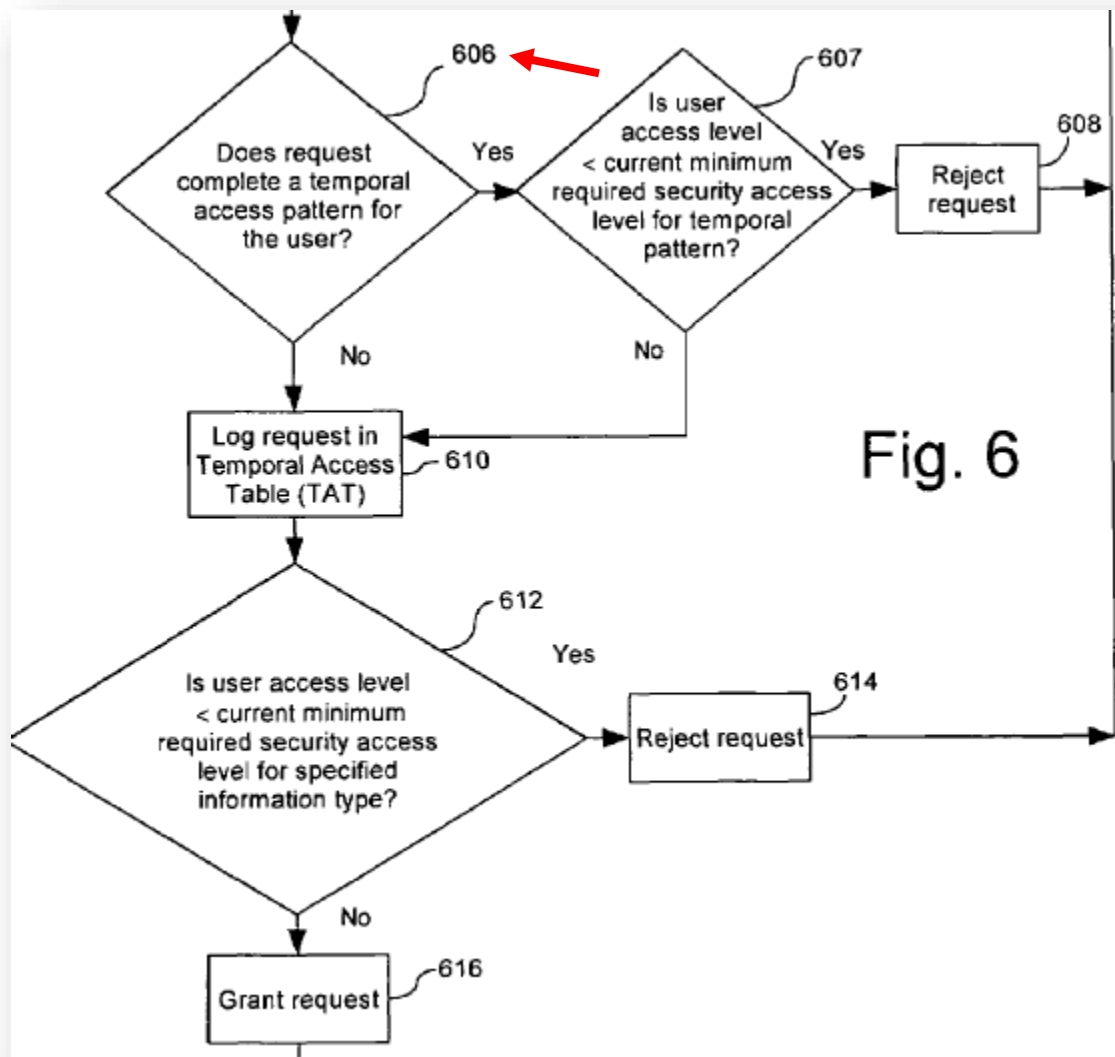
Petitioner addresses the “processing means” term of claim elements [10e-f], and claims 11 and 13-14 to the extent the Patent Owner argues or the Board finds it is governed by 35 U.S.C. § 112 paragraph 6 (“means-plus-function”). For each of the following functions of the “processing means,” the recited structure is a general purpose computer system adapted to carry out the algorithm(s) listed in the following sections (EX-1001 9:37-10:9; FIG. 10) and equivalents thereof (EX-1003 ¶¶46-52):

[10e] Function-1: comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity

Algorithm:

“The computer system determine if the access request completes a prohibited temporal access pattern for the entity.” EX-1001 1:62-64.

“[T]he system continues on to step 606 to determine if the request completes a temporal access pattern for the particular user”:



EX-1001 5:33-35, FIG. 6 (annotated).

“If the request does complete a temporal access pattern, this means that the sequence of operations performed matches an identified pattern.” EX-1001 5:36-37.

“Note that the temporal ordering of primitive access operations mandates that the operations occur in the order specified for the security policy to be

enforced. Thus, in FIG. 1, if 104₂ is accessed first followed by item 104₁, the security policy associated with node d, item 114₂, will not be activated because the temporal order was not satisfied.” EX-1001 5:42-47, *see also* FIG. 1.

“As shown in FIG. 4B, the Temporal Access Table maintains a history of the primitive operations performed by a user”:

Temporal Access Table (TAT)							
Usr	A	B	C	D	dir	exec	del
1(1)					102	112	
2(1)							
3(2)					111	103	
4(1)							
5(3)							

Fig. 4B

EX-1001 5:54-56, FIG. 4B.

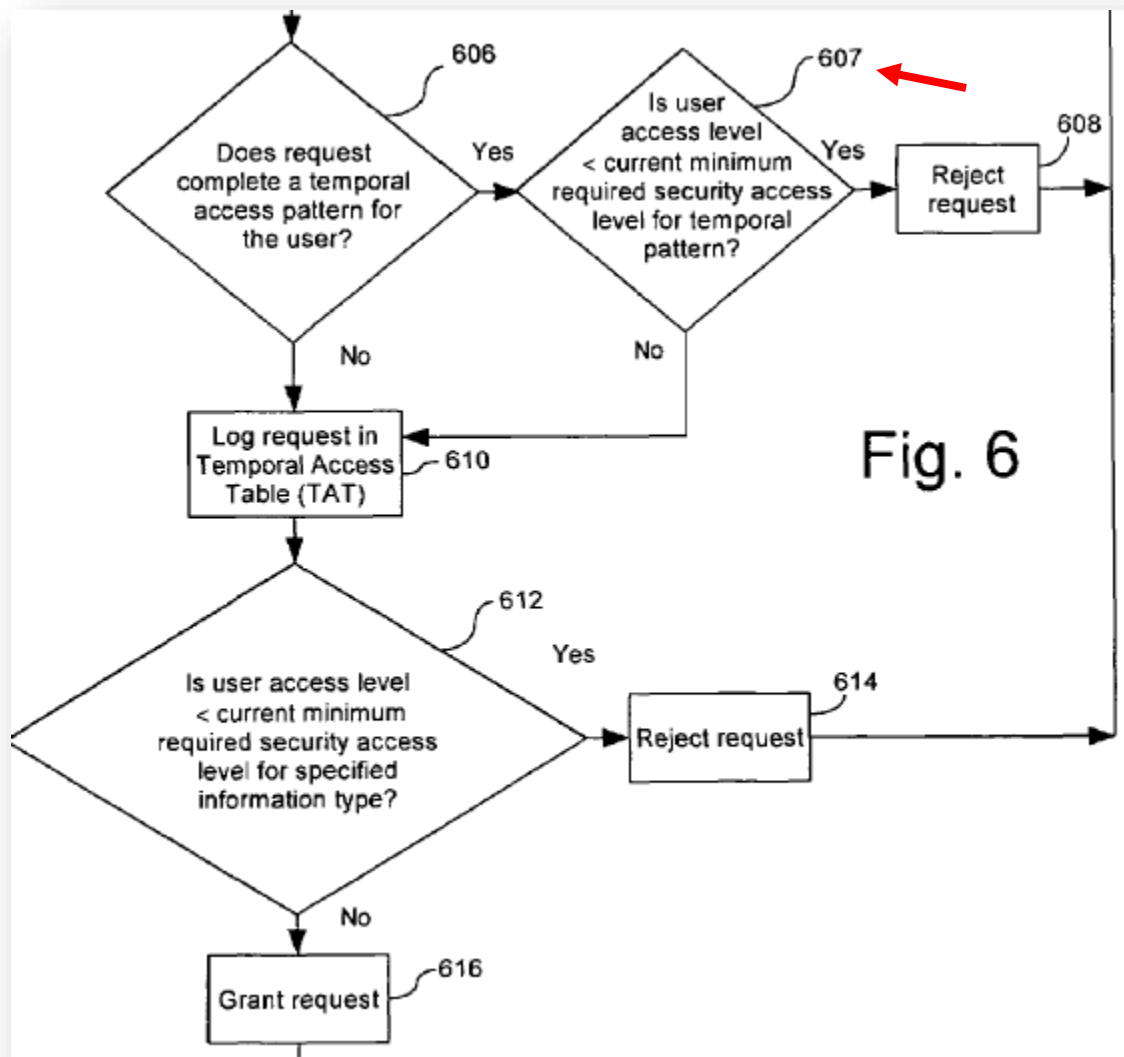
“As a user is granted authorization to perform a primitive access operation, the operation is time stamped and stored within the TAT. The time stamps are compared against the temporal patterns identified in the Temporal Order Table, FIG. 3, to check for matches”:

Temporal Order Table (TOT)							
TOT	A	B	C	D	dir	exec	del
a							
b							
c							
d					1	2	
e				1	2.1	2.2	3

EX-1001 5:56-60, FIG. 3.

To extent that the *a prohibited temporal access pattern* requires a comparison of *access levels*:

“If a temporal pattern is completed, the user’s access level is compared to the access level required for the requested access action, illustrated in step 607”:



EX-1001 5:39-42, FIG. 6 (annotated).

“If the access level of the user is not sufficient for the requested action, then the request is rejected in step 608.” EX-1001 5:47-49.

[10e] Function-2: comparing a minimum access level established for said first base node to said predetermined access level

Algorithm:

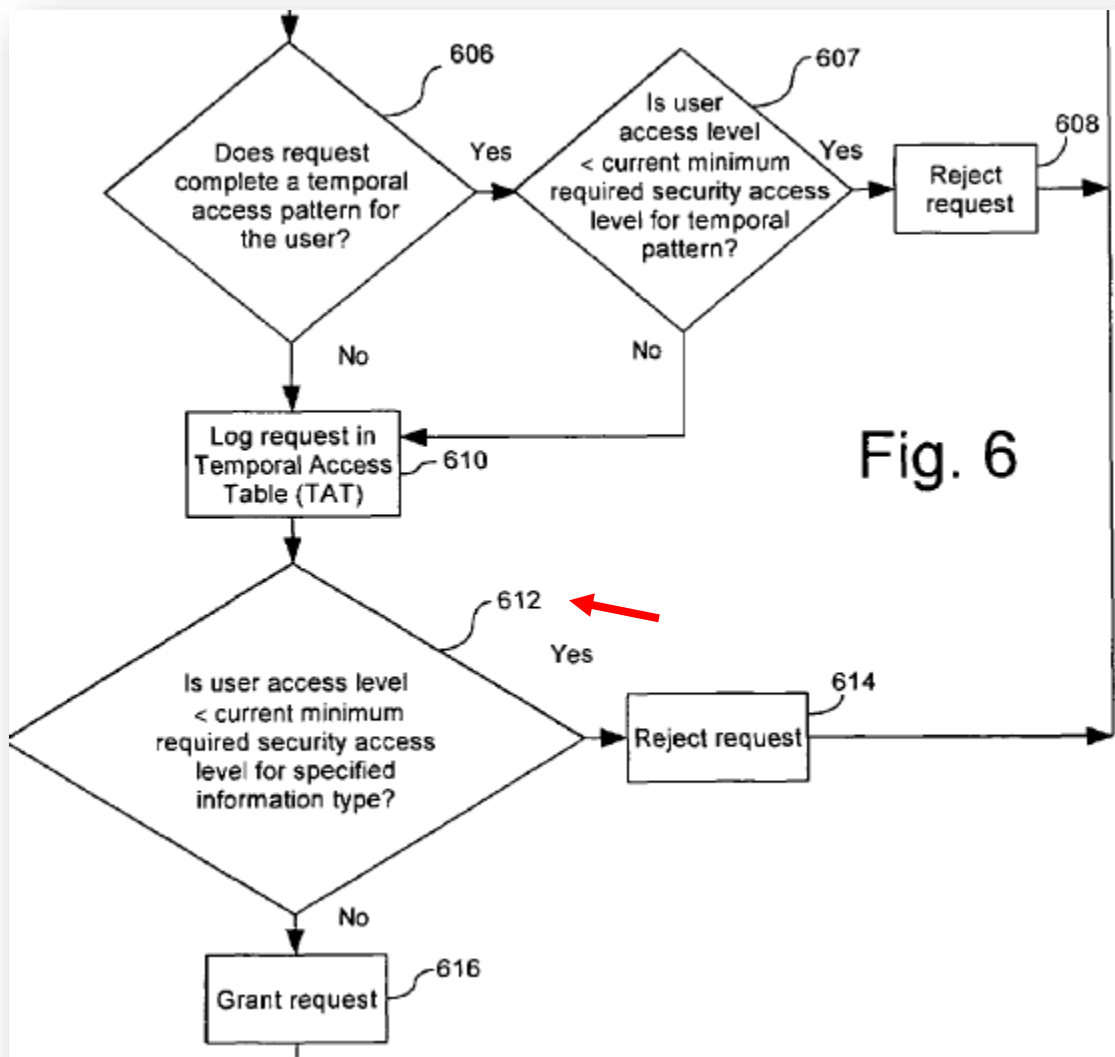
“The system also compares a minimum access level established for the first base node to the predetermined access authorization level assigned to the entity.”

EX-1001 Abstract.

“[T]he system can compare a minimum access level established for the first base node to the predetermined access authorization level assigned to the entity.”

EX-1001 1:65-67.

“In step 612,” of Figure 6 (below), “the computer system makes a determination as to whether the security access level of the user making the request is less than the current minimum required security access level for the specified information type.” EX-1001 6:2-8.



EX-1001 FIG. 6 (annotated).

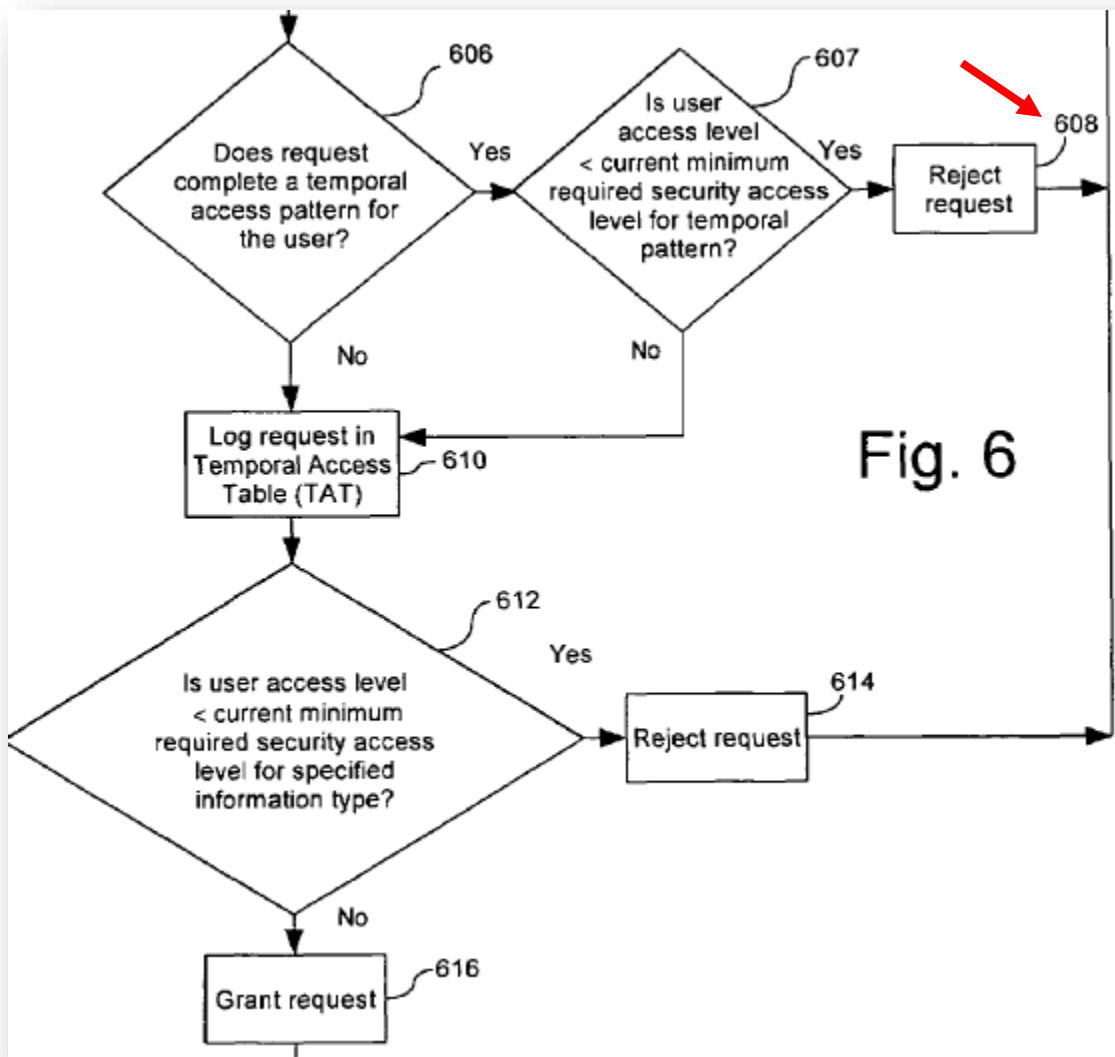
[10f] Function-1: denies said request if said access request completes a prohibited temporal access pattern for said entity

Algorithm:

“The computer system determine if the access request completes a prohibited temporal access pattern for the entity. If so, the request is rejected.” EX-1001 1:62-64.

“Note that the temporal ordering of primitive access operations mandates that the operations occur in the order specified for the security policy to be enforced. Thus, in FIG. 1, if 104₂ is accessed first followed by item 104₁, the security policy associated with node d, item 114₂, will not be activated because the temporal order was not satisfied.” EX-1001 5:42-47, *see also* FIG. 1.

“If a [prohibited] temporal pattern is completed,” then the request is rejected in step 608”:



EX-1001 5:39-49, FIG. 6 (annotated).

To extent that the *a prohibited temporal access pattern* requires a comparison of *access levels*:

“If the access level of the user is not sufficient for the requested action, then the request is rejected in step 608.” EX-1001 5:47-49.

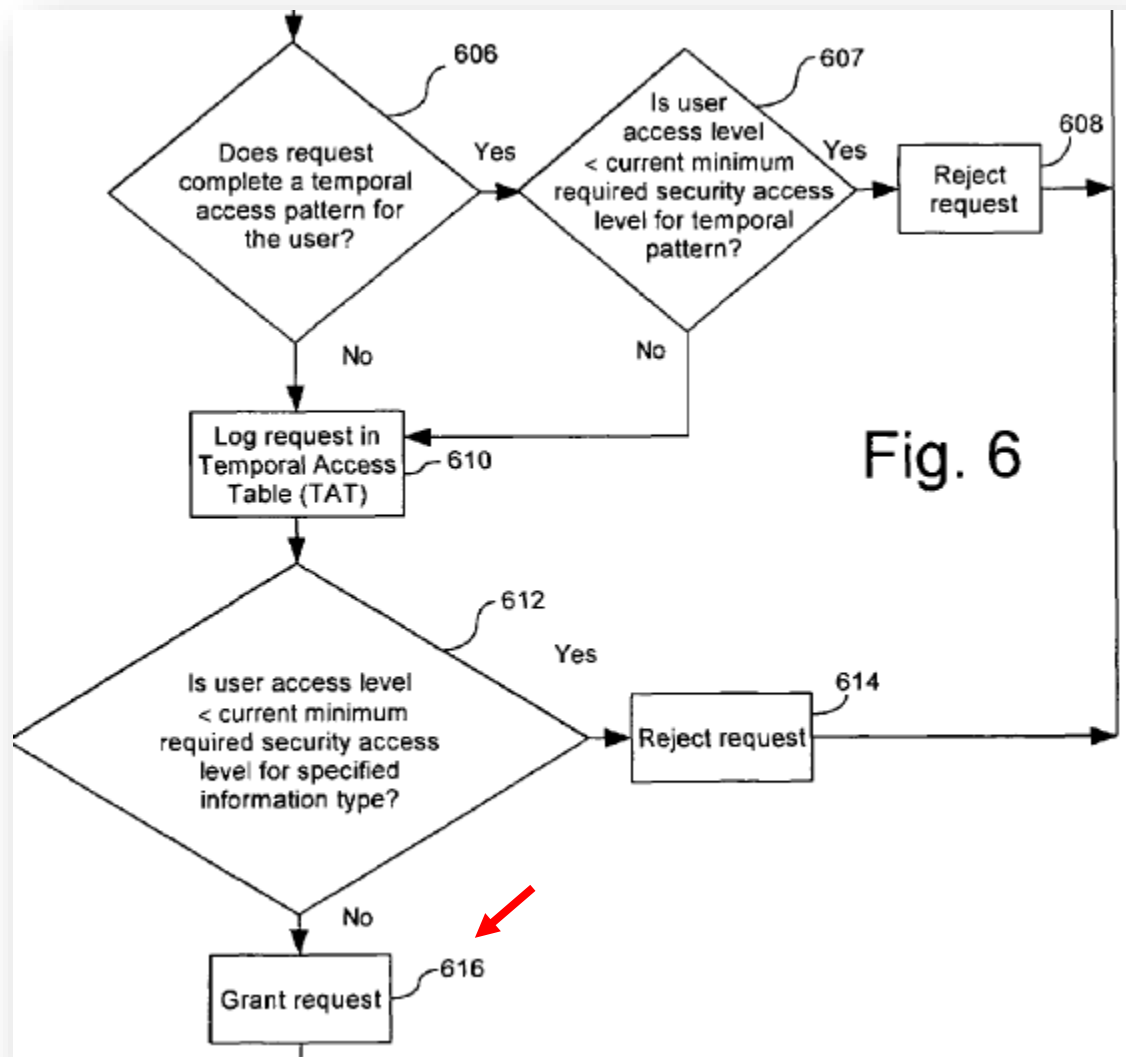
[10f] Function-2: grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level

Algorithm:

“If the request does not complete a [prohibited] temporal access pattern”
“then the system continues on to step 610 and logs the request in the Temporal Access Table (TAT). As shown in FIG. 4B, the Temporal Access Table maintains a history of the primitive operations **performed** by a user.” EX-1001 5:50-57.

“[T]he system can grant the access request only if the minimum access level for the first base node does not exceed to the predetermined access authorization level.” EX-1001 1:67-2:3

“[I]f the user does have a sufficiently high security access level then the request is granted in step 616”:



EX-1001 6:8-12, FIG. 6 (annotated).

To extent that the *a prohibited temporal access pattern* requires a comparison of *access levels*:

“If ... the user’s access level is sufficient for the temporal pattern completed, then the system continues on to step 610 and logs the request in the Temporal

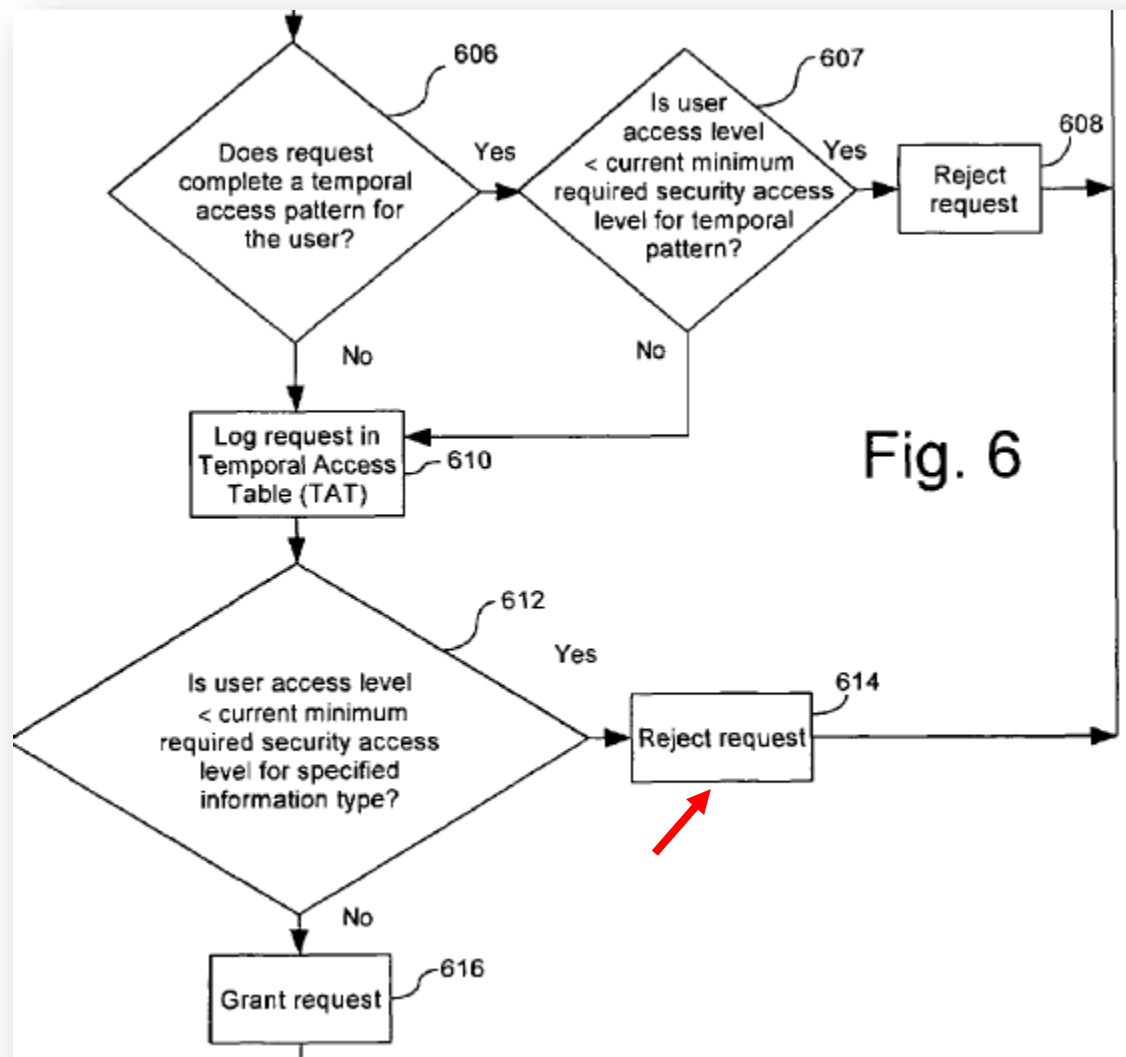
Access Table (TAT). As shown in FIG. 4B, the Temporal Access Table maintains a history of the primitive operations performed by a user.” EX-1001 5:50-57.

[11] Function: denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity

Algorithm:

“The method can also include the step of denying the request if the minimum access level for the first base node exceeds the predetermined access authorization level assigned to the entity.” EX-1001 2:3-6.

“If the user does not have authorization for at least the current minimum required security access level, then the request is rejected”:



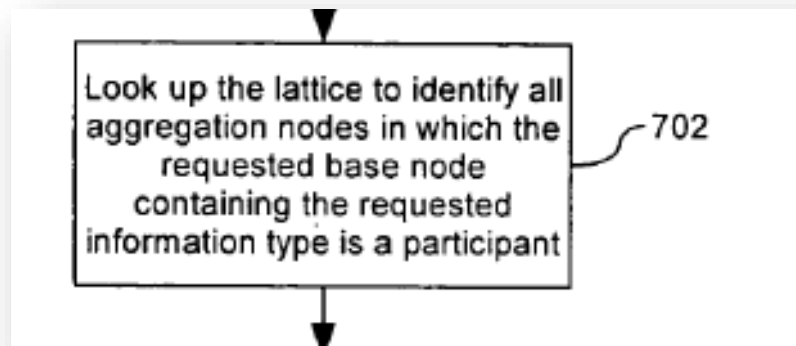
EX-1001 6:8-12, FIG. 6 (annotated).

[13] Function: identifies within said hierarchy any higher-level nodes that are aggregations comprising said first base node

Algorithm:

“[T]he method can include the step of identifying within the hierarchy any higher-level nodes that are aggregations comprising the first base node.” EX-1001 2:13-15.

“[T]he process can continue in step 702 of FIG. 7 by identifying all higher-level aggregation nodes 112 in which the base node containing the requested information type is a participant”:



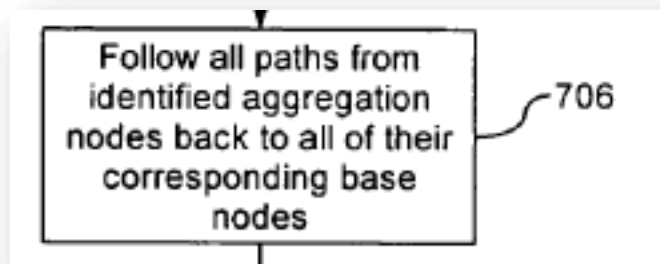
EX-1001 6:42-45, FIG. 7.

[14] Function: identifies within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node

Algorithm:

“The method can also include identifying within the hierarchy any nodes that directly or indirectly comprise children of any of the higher-level nodes that are aggregations comprising the first base node.” EX-1001 2:16-19.

“[I]n step 706 the computer system can identify all base nodes that are also participants in that particular aggregation node. This can be accomplished, for example, by following all paths from the identified aggregation nodes back to all of their corresponding base nodes”:



EX-1001 6:48-53, FIG. 7.

The prior art relied on in this Petition performs these functions using the structures described in the '708 Patent or equivalents thereof. Because the prior art discloses each claim term of the Challenged Claims under any reasonable construction, including if means-plus-function applies, the Board need not adopt any claim construction in order to determine that the Challenged Claims are obvious. EX-1003 ¶53.

D. Priority of the Challenged Claims

This Petition relies on prior art as of the earliest claimed priority date of the '708 Patent—its filing on March 11, 2004 (“Priority Date”). EX-1001 (21).

E. Person of Ordinary Skill in the Art

A Person of Ordinary Skill in the Art (“POSA”) in March of 2004 was familiar with computer-security and, in particular, access-control methods. EX-1003 ¶57. A POSA would have had at least a Bachelor’s degree in Computer Science, Computer Engineering, or a similar degree and at least two years of professional experience with computer systems, including computer-security and

access-control methods. More experience can supplement less education and vice versa. *Id.* The level of skill in the art is further demonstrated by the references cited herein, including the Grounds’ references and the background references discussed in the State of the Art section below. While this Petition, and supporting declaration, may occasionally use the present tense, the analysis is from the perspective of a POSA as of the time of the purported invention. EX-1003 ¶57.

F. State of the Art

This section describes the state of the art, including the general knowledge, skill, common sense, and creativity possessed by a POSA as of March 2004. It explains the conventional purposes and structures of conventional components in the art, informing the motivations and reasonable expectations of success for the Grounds. EX-1003 ¶¶58-68, 70-72.

1. Well-known sensitivity-based (i.e., “access levels”) access control methods

By March 2004, controlling computer access based on the sensitivity of the information and the authorization or “clearance” level of the requesting user was well known. EX-1003 ¶¶59-65.

For example, in 1985, the Department of Defense published the *Trusted Computer Evaluation Criteria* to “provide guidance to manufacturers” for their “widely-available” “commercial products” “for sensitive applications,” including “specific security feature requirements” that “encompass the capabilities typically

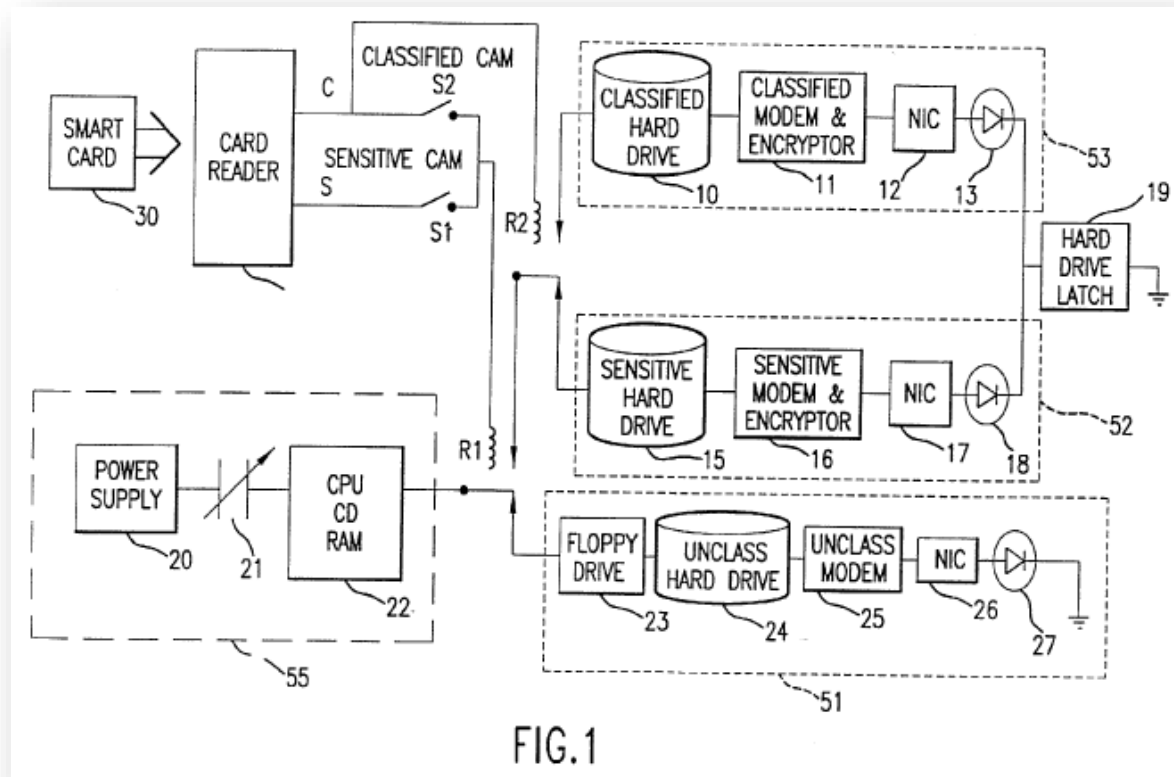
found in” “general-purpose operating systems.” EX-1013 6, 8. These features included a “security policy,” or “a set of rules that” “determine whether a given subject can” “gain access to a specific object.” EX-1013 9. As an example rule: “No person lacking proper personnel security clearance shall obtain access to classified information.” EX-1013 9. Such access control rules required using “[a]ccess control labels” “associated with objects” and knowing “what classes of information”—*e.g.*, “security level” and “hierarchical classification”—“[users] are authorized to deal with.” EX-1013 9-10, 65, 111. With such information, “a comparison of” a user’s “clearance/authorization to” “the classification/sensitivity designation of the information” is performed to determine whether to grant access. EX-1013 60. Knowing a user’s assigned “security level” required identification and authentication of that user. EX-1013 10, 62; EX-1003 ¶60.

These access control methods utilized a “reference monitor [that] enforces the authorized access relationships between subjects and objects.” EX-1013 65. Reference monitors were known to function as “an essential element of any system that would provide multilevel secure computing” “controls.” EX-1013 65. Such reference monitors were implemented by “security kernel(s).” EX-1013 65; EX-1003 ¶61.

There were also other well-known systems and methods for controlling access based on such “access levels,” including using the “classification/sensitivity

designation” as taught by *Trusted Computer Evaluation Criteria*. EX-1003 ¶62.

U.S. Pat. Appl. Pub. 2002/0147924A1 to Flyntz (“Flyntz”) (Ex-1014), published 2002, discloses a multilevel computer security system:



EX-1014 Abstract, FIG. 1. Following authentication, a user could “select one of the security levels” (e.g., “sensitive,” “classified,” etc.) of the system and, if the user is authorized for that security level, access is permitted through an electronically-activated switch that couples the computer 55 to the information subsystem (e.g., 51, 52, 53). See, e.g., EX-1014 [0032-37, 41], FIG. 1; EX-1003 ¶62.

Other prior art systems, as recognized by the '708 Patent, similarly provided access to information based on “security ranks”. EX-1001 1:33-38; EX-1003 ¶41. U.S. Patent No. 6,453,418 to Ooki et al. (“Ooki”) (EX-1007), published 2002, permitted access to user data based on the relative security ranks among users requesting and creating the data. EX-1007 Abstract, 2:5-9 (“an information accessing method that controls permission to access the user data according to corresponding **relation of a security rank between a user whose data is accessed and a user who would access the user data**”), 2:41-45, FIG. 3 (showing user security ranks). EX-1003 ¶63.

Ooki’s system was configured to set one of plural security ranks to each user, set a table for determining if the access to the user data is permitted from a security rank of a user for requesting the access to the user data and a security rank of a user whose data is accessed by the former user, and determine if the access to the user data is permitted by referencing this table. EX-1007 2:21-28. Each entry on this table was composed of a user ID 431 and a security rank 432:

FIG.3

430 USER ID TABLE		
431 USER ID	432 SECURITY RANK	433 ATTRIBUTE OF ANOTHER USER
C001	A	BELONGING, POSITION AND THE LIKE OF USER
C002	A	BELONGING, POSITION AND THE LIKE OF USER
C003	B	BELONGING, POSITION AND THE LIKE OF USER
C004	C	BELONGING, POSITION AND THE LIKE OF USER
C005	C	BELONGING, POSITION AND THE LIKE OF USER
B001	C	GUEST
B002	D	GUEST

EX-1007 4:23-26, FIG. 3. Ooki disclosed that “the top rank is A and the rank goes down” “from A to Z” and “if (the security rank of the user who wants to access the data)” is less than or equal to “(the security rank of the user whose data is to be accessed), the user who wants to access the data is” “permitted to access the data, while if not, he or she is not permitted to access.” EX-1007 4:38-51. Ooki’s comparison of the relative security ranks (“access levels”) to make access control decisions is but “an example of a **common** security management” technique well known before the ’708 Patent. *Id.*; EX-1003 ¶64.

It was also well known in the prior art that “access levels” of objects would vary based not only on the type of information, but also due to the aggregation of

information. EX-1003 ¶65. *Cryptography and Data Security* (EX-1016), published in 1982, recognized that “[a]n **aggregate** of data might require a **higher classification** than the individual items. This is because the **aggregate** might give an **overall picture** that cannot be deduced (or easily deduced) from an individual item.” EX-1016 017. This corresponds to the ’708 Patent’s statements regarding aggregated data and the heightened sensitivity of aggregated information, which was well known in the prior art:

aggregation nodes will **often** have a higher minimum required security level for permitting access as compared to security levels required for access to participant information types and/or system functions that comprise base nodes 110. This is true because **aggregated data is often of a more sensitive** nature since it provides **greater context** and can identify relationships between the various individual information types. Consequently aggregated information **will inevitably** be of greater interest to unauthorized users and system administrators **will naturally** wish to impose higher level restrictions on its access.

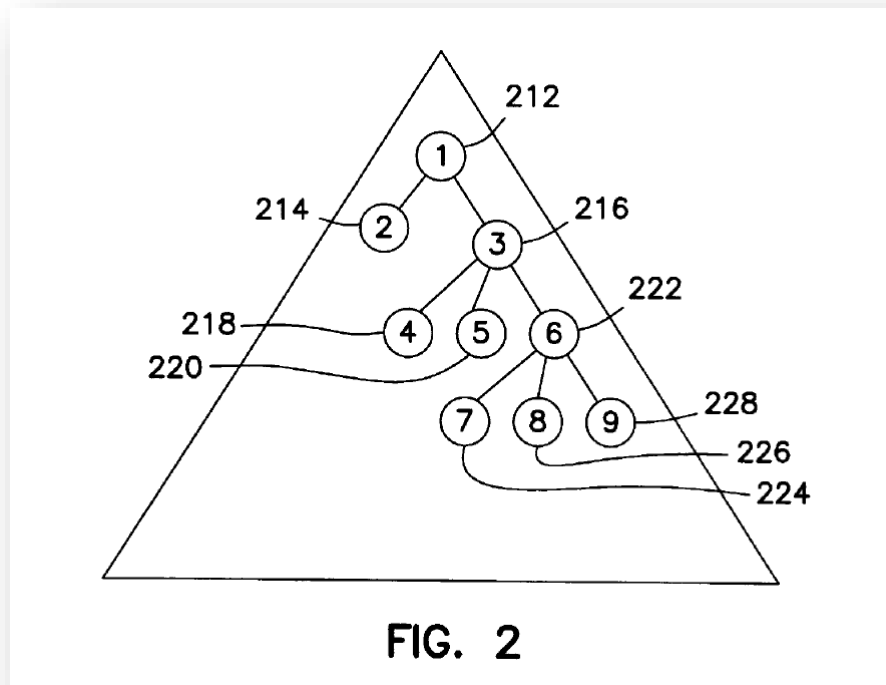
EX-1001 6:16-27; EX-1003 ¶65.

Thus, “*comparing a minimum access level established for said first base node to said predetermined access level*” as part of an access control decision was well known prior to the ’708 Patent and is nothing more than a “simple relational comparison.” EX-1001 1:24-27; EX-1003 ¶66.

2. Well-known method of organizing data: aggregation of nodes in a tree hierarchy

By March 2004, logically organizing computer data in the form of a tree hierarchy having a plurality of leaf nodes and higher-level nodes and the aggregation of nodes was well known, including in methods and systems for ensuring secure access to computer systems. EX-1003 ¶¶67-68.

U.S. Patent No. 6,446,077 to Straube et al. (EX-1008), issued 2002, involved aggregation of nodes in the form of a tree structured database 210 representing relationships between multiple objects on a storage domain. EX-1008 5:11-14, FIG. 2. A top level object 212 was represented by a “1” in a circle. A second object 214 was a child of the first object, as was a third object 216. The third object 216 had three children, 218, 220 and 222 and object 222 had three child objects 224, 226, and 228. EX-1008 5:21-26, FIG. 2; EX-1003 ¶68.



3. Well-known use of patterns of behavior/temporal access patterns in computer security and access control

By March 2004, the use of patterns of behavior and temporal access patterns for controlling access was well known. EX-1003 ¶¶70-72. U.S. Patent No. 6,334,121 to Primeaux et al. (“Primeaux”) (EX-1010) involved authenticating users using a set of security rules to track user usage patterns and flag suspicious activity on the system. EX-1010 Abstract, 1:15-20, 2:42-43 (“limiting the ability of unauthorized users to disrupt system operations by monitoring and reporting abnormal user usage patterns”). The system monitored a user’s patterns of commands/requests for system access and prevented users from executing destructive commands by detecting unusual patterns in their usage of the system.

EX-1010 2:58-60. The system learned a user's usage patterns and integrated the usage patterns with the security rules to recognize "normal" usage patterns for a particular user. When the user's commands did not follow the normal usage pattern, the commands used were checked against the system's security rules. EX-1010 2:63-3:1. When the system detected a usage pattern outside of the user's normal usage pattern, it triggered the system "to react automatically." EX-1010 10:60-67, Abstract ("perform[ing] automatic responses when confronted with non-authenticated users"). Thus, contrary to statements in the '708 Patent, Primeaux did not merely flag patterns of behavior (EX-1001 1:46-51), but enforced access control policies based on the detected patterns of behavior such as by "automatically log[ging] off the intruder or effect[ing] some other more severe reaction" and "automatically performing a predetermined action" such as "excluding [a] user from further system access." EX-1010 10:41-45, 12:1-16; EX-1003 ¶70.

Lane et al.'s, *Sequence Matching and Learning in Anomaly Detection for Computer Security*, ("Lane") (EX-1011), published 1997, described another computer security system known in the art that involved detecting unauthorized users based on a sequence of user actions and determining whether the sequence of actions was normal or anomalous. EX-1011 43, 44 (identifying "characteristic patterns of actions" and "us[ing] the sequence (an ordered, fixed-length set of

temporally adjacent actions) as the fundamental unit of comparison”). The system learned a user’s profile and based on sequences of actions (e.g., UNIX commands) by the user, the system determined whether the user’s current behavior was consistent or anomalous with past behavior. EX-1011 43; EX-1003 ¶71.

One other prior art system employed a method of controlling access to a computer system by determining whether an “attribute” of a use (i.e., a request to use an application or access a file) of that system matched one of either an allowed or disallowed use. These “[P]redefined attributes” included an “Action Flow” comprising a “sequence of actions.” Ben-Itzhak (EX-1012) [0001, 50-53, 60, 66, 126]; EX-1003 ¶72.

V. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 10-14 of the ’708 Patent are challenged in this Petition.

B. Statutory Grounds for Challenges

The Challenges are set forth in detail below and summarized as follows:

Ground	Claims	Basis	Reference
1	10-14	§ 103	Gladstone (EX-1004) in view of Salazar (EX-1009)

C. Prior Art Basis

U.S. Patent 7,290,266 to Gladstone et al. (“Gladstone”) (EX-1004), titled “Access Control by a Real-Time Stateful Reference Monitor with a State

Collection Training Mode and a Lockdown Mode for Detecting Predetermined Patterns of Events Indicative of Requests for Operating System Resources Resulting in a Decision to Allow or Deny Activity Identified in a Sequence of Events Based on a Rule Set Defining a Processing Policy” was filed Feb. 8, 2002 and issued Oct. 30, 2007, qualifying as § 102(e) prior art. EX-1004 (10, 22, 45, 54, 75). Gladstone was not cited or applied by the Examiner during the ’708 Patent prosecution. EX-1001 (56); EX-1002.

U.S. Patent Application Publication No. 2004/0122792 to Salazar (“Salazar”) (EX-1009) titled “Method, System, and Program Product for Managing Access to Data Items in a Database” was filed Dec. 20, 2002 and published June 24, 2004, qualifying as § 102(e) prior art. EX-1009 (10, 22, 43, 54, 75). Salazar was not cited or applied by the Examiner during the ’708 Patent prosecution. EX-1001 (56); EX-1002.

VI. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 10-14 Are Obvious Over Gladstone (EX-1004) and Salazar (EX-1009)

1. Gladstone

a. Analogous Art

Gladstone is analogous art to the claimed invention. For example, the field of endeavor of the ’708 Patent’s claimed invention is “generally [directed] to

computer and information security and more particularly to security measures that enforce security based on logical”—*i.e.*, software—“implementation methods.” EX-1001 1:8-11, 19-21; EX-1003 ¶78. The ’708 Patent’s stated solution uses a “temporal access pattern” in access control decisions to ensure “secure access to a computer system.” EX-1001 1:55-2:6, Claims 1, 9, 10. The ’708 Patent contrasts this solution with the well-known “simple relational comparison” and “point tests” of conventional “logical security safeguards [that] typically provide access based on a user/group/role identifier and an access control list for the file, database, or system function,” faulting (incorrectly, §IV.F.3) the art for not “enforc[ing] security based on patterns of behavior,” *i.e.*, “temporal patterns of access.” EX-1001 1:22-51; EX-1003 ¶78.

Gladstone is in the same field of endeavor as the ’708 Patent because it is directed to systems and methods for controlling security policy of a computer system. EX-1004 3:46-48, Title; EX-1003 ¶79. These systems and methods used, *inter alia*, software “logic” within a stateful reference monitor. EX-1004 5:57-60. Like the ’708 Patent, Gladstone acknowledges the well-known “common scenario” of “control[ling] access to various system resources” “for purposes of securing a system against deliberate and malicious attack” and the limitations of such access control techniques. EX-1004 1:39-42, 3:11-16; EX-1003 ¶79. These “common” solutions control access to “system resources” that include “files” and various

“network connections,” “system call functions,” etc. (*i.e.*, computer system functions). EX-1004 1:22-25; 10:9-3; EX-1003 ¶79.

Gladstone is reasonably pertinent to the problem addressed by the ’708 Patent’s claimed invention because its solution, like the ’708 Patent’s, provides access control to such resources “based on a pattern of activity,” “prohibited pattern[s],” “behavior,” “anomalous behavior,” “combination[s] of events,” and, specifically, “a particular **sequence of events**.” EX-1004 Title, Abstract, 2:3-4; 4:46-65, 6:13-24, 9:11-27, 9:54-55, 11:1-3, 11:63-65, 13:8-17, Claims 1, 8-10; EX-1003 ¶80.

a. Overview of Gladstone

Gladstone is directed to a system and method for controlling a security policy of a computer system. EX-1004 3:46-48. Gladstone discloses that an “important aspect of system security is monitoring system events 100, e.g. access requests to a resource, and controlling the effect of those events, e.g. blocking or allowing the requested access to a resource.” EX-1004 5:6-9. To effect this access control, events 100 are “communicated to a stateful reference monitor 104” that makes decisions to allow or block the event. EX-1004 5:9-24. The stateful reference monitor operates by “correlat[ing] the access requests for a number of different resource types-files, system configuration information, network access, system calls, local or remote object invocation, etc.” EX-1004 9:43-55. Gladstone

describes that this “comprehensive view” “enables the stateful reference monitor 104 to make better access control decisions than a conventional, single resource type stateless reference monitor.” EX-1004 9:50-53; EX-1003 ¶81.

Correlating access requests enables Gladstone’s stateful reference monitor to “detect[] anomalous behavior and prevent further access.” EX-1004 9:54-55. If “a prohibited combination of events” were “X-Y-Z”—each a separate event (access request), i.e. “Event X, Event Y and Event Z”—a rule would prohibit Event Z if Event X and Event Y occurred within a prescribed timeframe of one another. EX-1004 6:13-19. Gladstone’s access control decisions are not made merely on the basis of generic combinations of events (access requests). Rather, Gladstone also describes policies controlling “patterns of events” and “pattern(s) of activity” that protect against “prohibited” or “unsafe” access requests. EX-1004 9:11-14, Claims 1, 8-10. Gladstone describes that such pattern-based determinations utilize a “collection of information, that is collected in real-time, indicative of a condition of a machine or process as a result of a particular sequence of events leading to the condition.” EX-1004 2:1-3:42. Gladstone explains that using the “particular sequence of events leading to the condition” is a key distinction between its stateful reference monitor and prior art “stateless reference monitors” that “control[] access to resources” in different ways. EX-1004 2:1-3:42. Gladstone does not, however, disregard the use of stateless monitors, stating that its “stateful

reference monitor 104 acts as an additional processing step over and above any existing stateless reference monitor in the operating system. Thus, [stateful reference monitor 104] cannot grant access when the standard stateless reference monitor would have denied access.” EX-1004 10:48-52; EX-1003 ¶82.

Thus, Gladstone discloses the same solution as the ’708 Patent—access control decisions utilizing particular sequences of events. EX-1003 ¶83.

2. Salazar

a. Analogous Art

Salazar is analogous art to the claimed invention. The field of endeavor of the ’708 Patent’s claimed invention is “generally [directed] to computer and information security and more particularly to security measures that enforce security based on logical”—*i.e.*, software—“implementation methods.” EX-1001 1:8-11, 19-21; EX-1003 ¶84. Although the ’708 Patent uses a “temporal access pattern” to distinguish the “simple relational comparison[s]” of prior art systems, it nevertheless incorporates such features into its claimed solutions, *e.g.*, by “comparing a minimum access level established for said first base node to said predetermined access level [of said entity].” EX-1001 Abstract, 1:21-51, 1:55-2:6, Claims 1, 9, 10. Further, the ’708 Patent claims “logically organizing said computer system in the form of a **tree hierarchy** having a plurality of **leaf nodes** and **higher-level nodes**”:

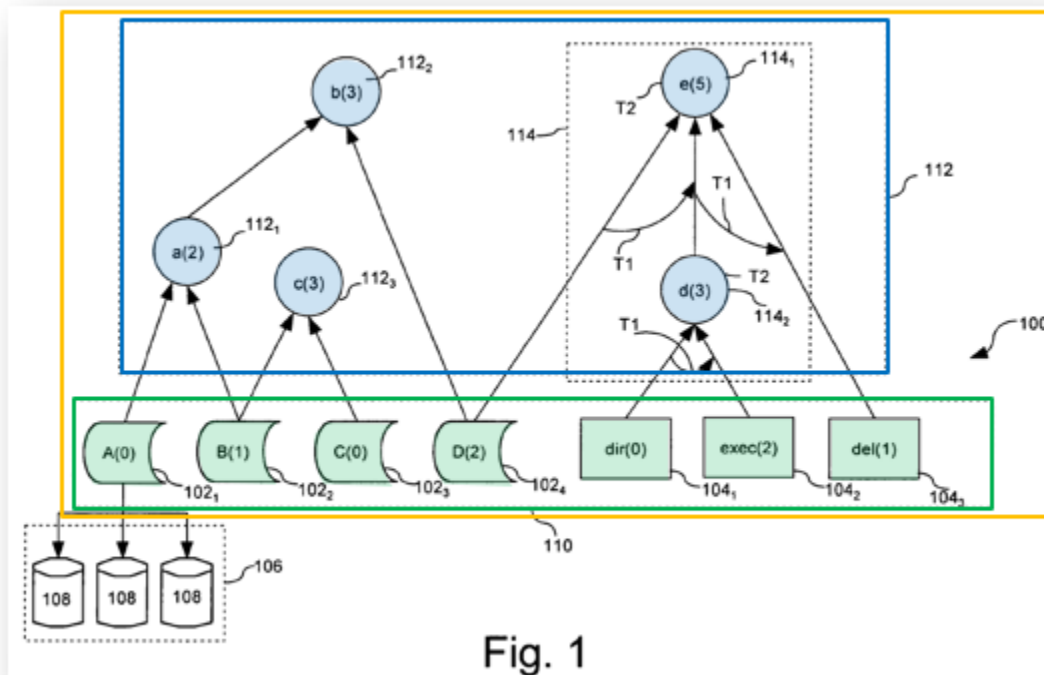
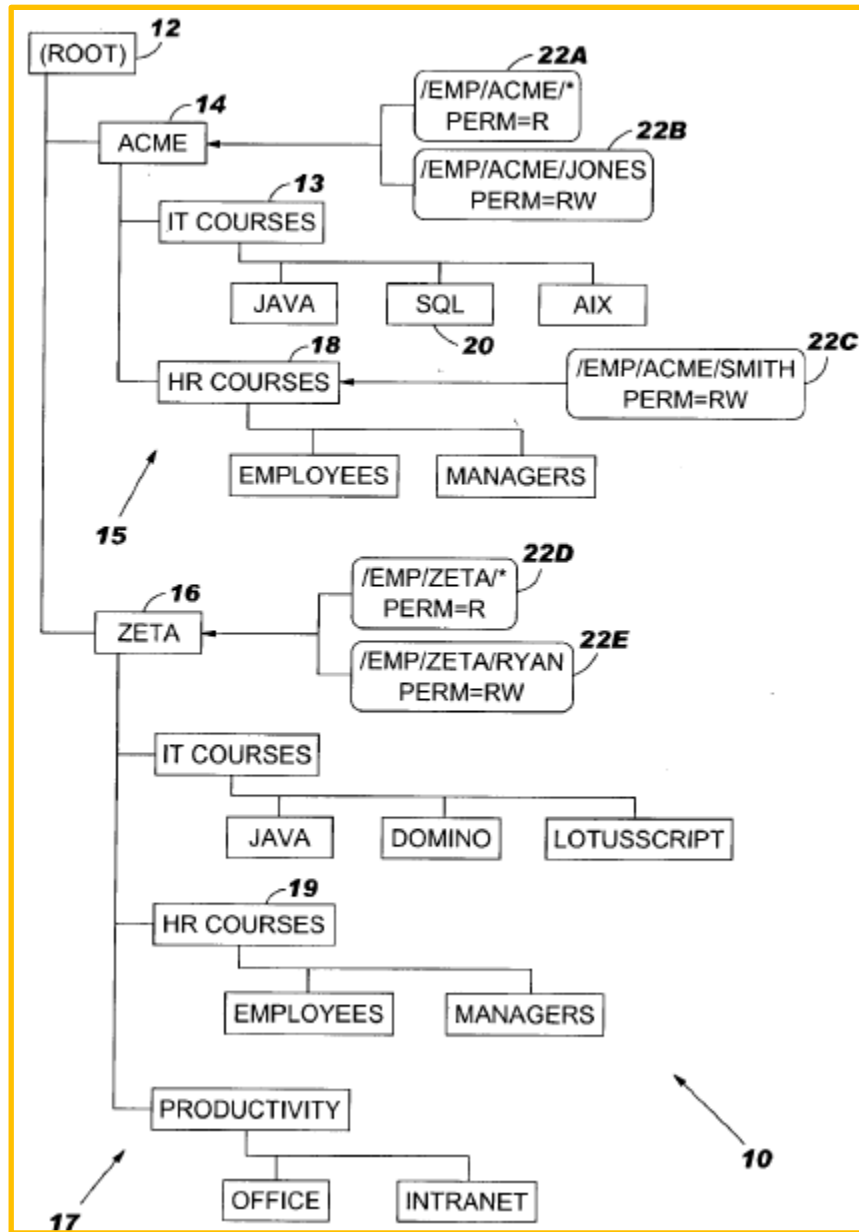


Fig. 1

EX-1001 Claims 3, 9, 10, 3:42-51, FIG. 1 (annotated); EX-1003 ¶84.

Salazar is in the same field of endeavor as the '708 Patent because it is directed to computer and information security by “manag[ing] access to data items.” EX-1009 Abstract, [0002]. Salazar is reasonably pertinent to the problem addressed by the '708 Patent’s claimed invention because, like the '708 Patent, Salazar performs the “simple relational comparison” by “matching one or more particular user properties associated with a user requesting the access to a user property in an access entry.” EX-1009 Abstract, [0007]. Salazar’s “data items” are also, like the '708 Patent, “arranged into a **[tree] hierarchy** of nodes”:

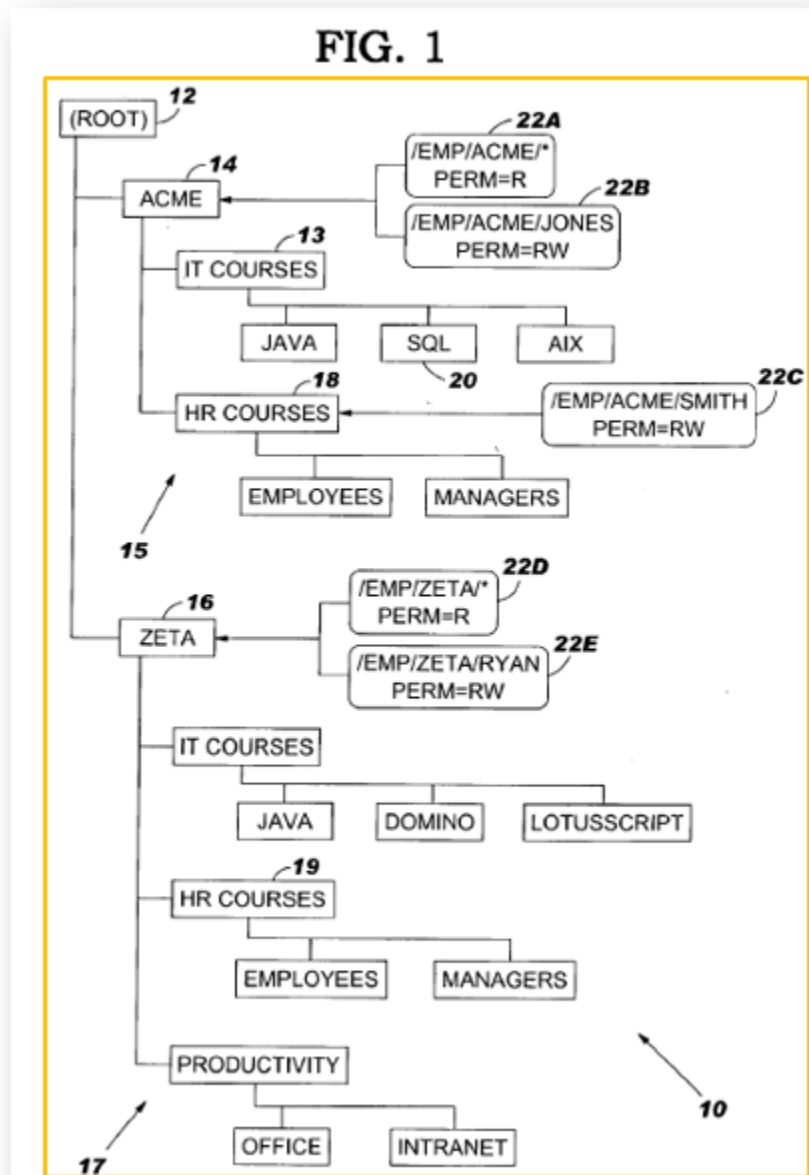
FIG. 1



EX-1009 [0002, 7, 20-23, 42], FIG. 1 (annotated); EX-1003 ¶85.

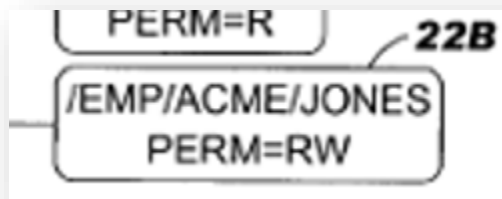
b. Overview of Salazar

Salazar discloses systems and methods for managing access to data items in a database arranged into **a hierarchy of “nodes”** (e.g., root node 12, ACME node 14, IT COURSES node 13, SQL node 20, etc.):



EX-1009 (54), Abstract, [0002, 7], FIG. 1 (annotated). Hierarchy 10 contains “parent” nodes and “child” nodes, *e.g.*, root node 12 is a parent to both ACME node 14 and Zeta node 14. EX-1009 [0020-21]. Thus, “parent” nodes “can be used to combine”—or aggregate—“child node[s],” including child nodes that form “the top node (or root node) of” another “hierarchy.” *Id.* “[C]hild nodes” form “the lowest level of the hierarchy.” *Id.*; EX-1003 ¶86.

Salazar associates “access entries,” *e.g.*, access entries 22A-E, with various nodes of hierarchy 10 as shown in Figure 1. EX-1009 [0024], FIG. 1. Each access entry 22A-E associates a “user property” with what Salazar describes as an “access level.” EX-1009 [0024]. The user property may be position (employee “EMP”), division (“ACME”), and user (“JONES”) or combination thereof—*i.e.*, “/EMP/ACME/JONES”—and the “levels of access” can be particular operations that are to be performed (*e.g.*, read only, read/write). EX-1009 [0023-25]. Access entry 22B associates the user property “/EMP/ACME/JONES” with a “read/write” access level (*i.e.*, “PERM=RW”):



EX-1009 [0027], FIG. 1; EX-1003 ¶87.

When a user requests data items and/or attempts to perform an operation on data items, access is allowed, or not, “based on one or more particular user properties [that are] associated with user” and, separately, included in “the access entries.” EX-1009 [0030-31]. User properties are provided to an access system that separately obtains the access entries (*e.g.*, 22A-E) that then “determines the access level of user” “based on the one or more access entries that are **matched** with [the] user” using the property associated with the user and the access entry. EX-1009 [0032-34]; EX-1003 ¶88.

Salazar discloses that these “user properties” broadly cover any property or characteristic that may be associated with a requesting user. Salazar discloses that the “user property can be **any** property associated with a set of users such as a path/directory, a group designation, a user attribute, etc.” EX-1009 [0024]. This includes both a “group specific property or a personal property associated with [the] user.” EX-1009 [0029] (internal quotes omitted). User properties further include, for example, a user’s department, country, or role. EX-1009 [0034] (“Dept=ACME and Country=USA,” “isManager”); EX-1003 ¶89.

Therefore, Salazar discloses granting access based on a comparison of user properties to required user properties identified by access entries associated with various nodes within the tree hierarchy. EX-1003 ¶90.

3. Motivation to combine Gladstone and Salazar

A POSA would have been motivated to combine Gladstone's systems and methods with Salazar's tree hierarchy of nodes and user-property-driven access control decisions to achieve more efficient implementation of access control across a tree hierarchy of nodes and fine-tuning access control capability. EX-1003 ¶91. Salazar states that "hierarchy of nodes 10 is **useful** in categorizing data items so that they can be **efficiently** located and retrieved." EX-1009 [0023]. Salazar discloses that its method of associating its access entries with the nodes "provides a more **flexible**, and **efficient** implementation of managing access to data items arranged into a hierarchy of nodes." EX-1009 [0007]. A POSA would have recognized that such a tree structure would improve performance and storage efficiency of the access control system and method described by Gladstone that was used for many and a variety of resources. EX-1003 ¶91. Salazar discloses that its methods "perform access control at an application level,"—*e.g.*, a database—"based on a user identification or other **user property**" and that "[m]anaging access control at this level allows applications to **fine-tune** the access-control scheme to their needs." EX-1009 [0005]. A POSA would have recognized Salazar as describing the details of a stateless reference monitor as described by Gladstone, and would have recognized that this fine-tuning of access control would benefit

Gladstone's system of implementing access control based on sequences of events at the user level. EX-1003 ¶91.

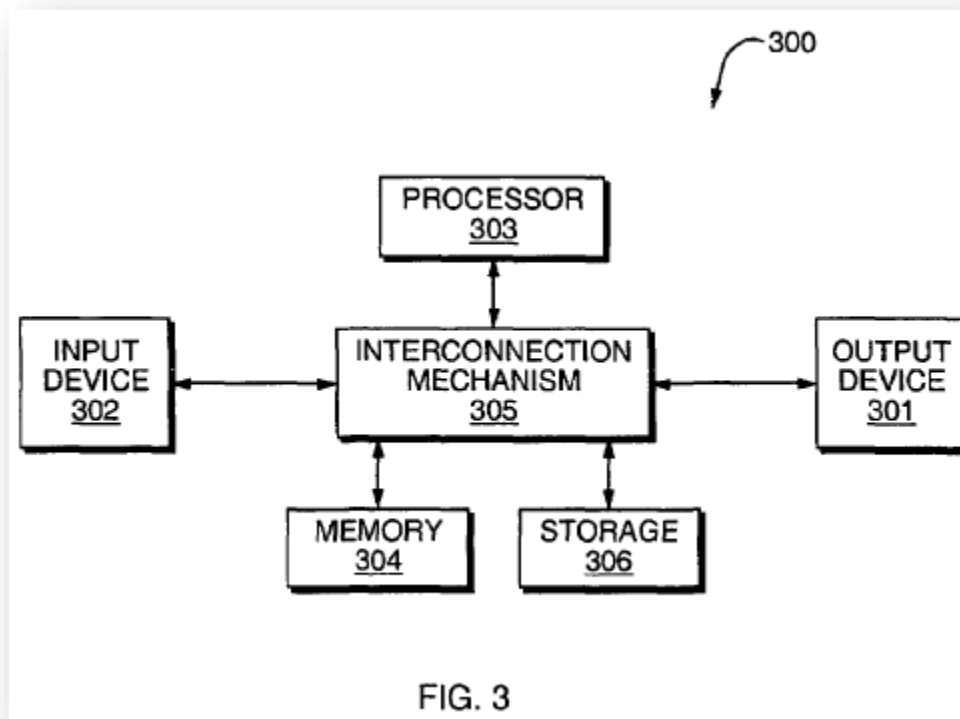
4. Detailed Application to the Challenged Claims

a. Claim 10

[10pre] A secure computer system comprising:

To the extent the preamble is limiting, Gladstone discloses implementing a security policy on computer system 300 (*a secure computer system*). EX-1003 ¶139.

Gladstone discloses “controlling an operating policy of a computer system, such as a security policy.” EX-1004 3:46-48. Gladstone states that an “important aspect of system security is monitoring system events 100, e.g. access requests to a resource, and controlling the effect of those events, e.g. blocking or allowing the requested access to a resource.” EX-1004 5:6-9. Gladstone implements these methods for “computer system 300, shown in FIG. 3”:



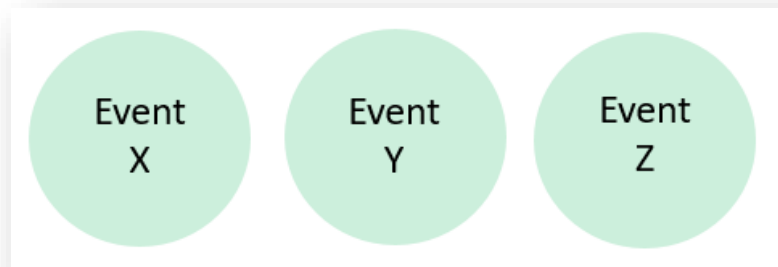
EX-1004 4:57-59 (“FIG. 3 is a functional block diagram of a hardware system on which the software system of FIGS. 1 and 2 can execute”), 14:20-15:12, FIG 3; EX-1003 ¶140.

Thus, Gladstone discloses *a secure computer system*. EX-1003 ¶141. Gladstone’s *secure computer system* comprises the elements [10a]-[10f] as discussed below. EX-1003 ¶141.

[10a] a plurality of logical base nodes representing at least one of an information type and a computer system function;

Gladstone discloses making access control decisions for various types of resources (*a plurality of logical base nodes representing at least one of an information type and a computer system function*). EX-1003 ¶142.

Gladstone discloses “a number of different resource types—files, system configuration information,”—*i.e.*, *information type[s]*— and “network access, system calls, local or remote object invocation, etc.”—*i.e.*, *computer system function[s]*. EX-1004 9:43-55, 10:9-47 (describing various computer system functions and acknowledging that other functions and resources may need protecting); 6:16 (referencing generic resource requests as “Event X, Event Y and Event Z”); 6:64-7:3 (resources include “Outlook personal address books.”); EX-1003 ¶143. Each of these examples, *e.g.*, “Event X, Event Y and Event Z,” is a base node:



EX-1003 ¶143.

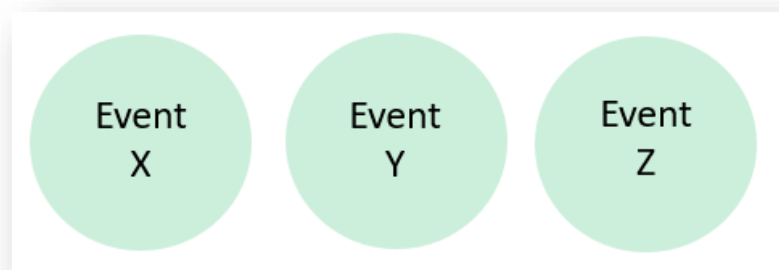
Gladstone’s methods determine “an action” for stateless reference monitor “to take, such as allowing” “or not allowing” “an access request.” EX-1004 5:20-24. Therefore, Gladstone discloses access control decisions for various types of resources (*a plurality of logical base nodes representing at least one of an information type and a computer system function*) consistent with the description

of the '708 Patent. EX-1001 2:67-3:2 (“The security access primitives can form base nodes in the hierarchical, directed graph.”), 3:46-47 (“object types and system functions can be defined as” “leaf or base nodes 110”), 3:64-66 (describing “nodes” as “representing information access and operational functions for which the security operations are to be enforced”); EX-1003 ¶144. Further, Gladstone discloses that its systems and methods used “logic” and, therefore, a POSA would understand that the resources to which access is controlled are “*logical*.” EX-1004 5:57-60; EX-1003 ¶144.

[10b] a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy;

Gladstone discloses, or renders obvious alone or in combination with Salazar, this limitation. EX-1003 ¶¶145-149.

As described above in [10a], Gladstone discloses *base nodes* “Event X, Event Y and Event Z”:



See [10a]; EX-1003 ¶146.

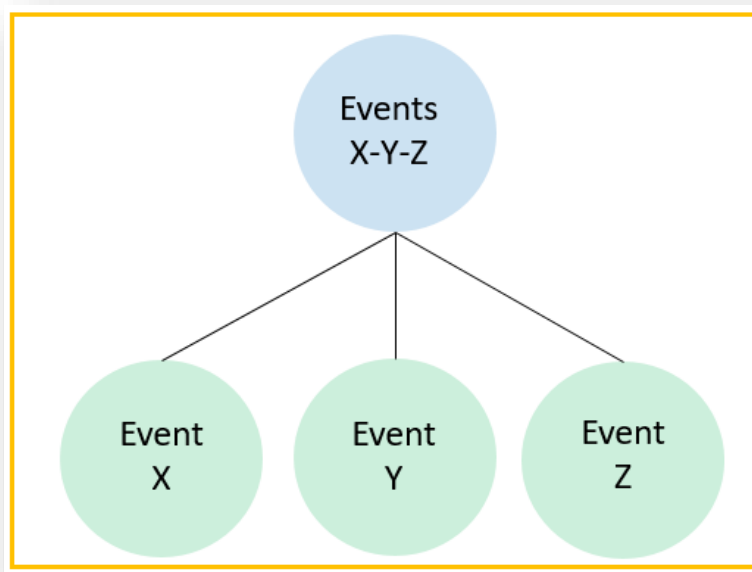
Gladstone further describes access control decisions based on the combined occurrence of each of Events “X,” “Y” and “Z” within a certain timeframe. For example, a “prohibited combination of events” of “X-Y-Z” would “prohibit Z” if the request for Event Z occurred while “state database 207 holds information X-Y”—indicating that events X and Y had already occurred. EX-1004 6:13-14. A POSA would have understood that such a combination of base nodes:



is a *higher-level node* as described by the 708 Patent. EX-1001 3:2-6 (“Higher level nodes within the graph represent information aggregation sets and/or temporal patterns of access.”); EX-1003 ¶147. A POSA would have also found it obvious to include other higher-level nodes where needed as a mere duplication Gladstone’s express example. EX-1003 ¶147. Therefore, Gladstone discloses a *plurality of higher-level nodes*. EX-1003 ¶147.

A POSA would have understood that Gladstone discloses, or at least found it obvious, that Gladstone’s *plurality of higher-level nodes* and *said base nodes* were *arranged together... in the form of a tree hierarchy*. EX-1003 ¶148. For example, Gladstone’s description of the separate requests of Events X, Y and Z and the

prohibited combination of X-Y-Z described a deliberate, knowing relationship between the individual events and the combined event. EX-1004 6:13-19. A POSA would have understood, or at least found obvious, to organize such information in the typical fashion—including in the computer security space—of using a *tree hierarchy*. EX-1003 ¶148 (§V.F.2); §IV.F.2. Thus, a POSA would have understood *plurality of higher-level nodes* and *said base nodes* were arranged *together... in the form of a tree hierarchy*:

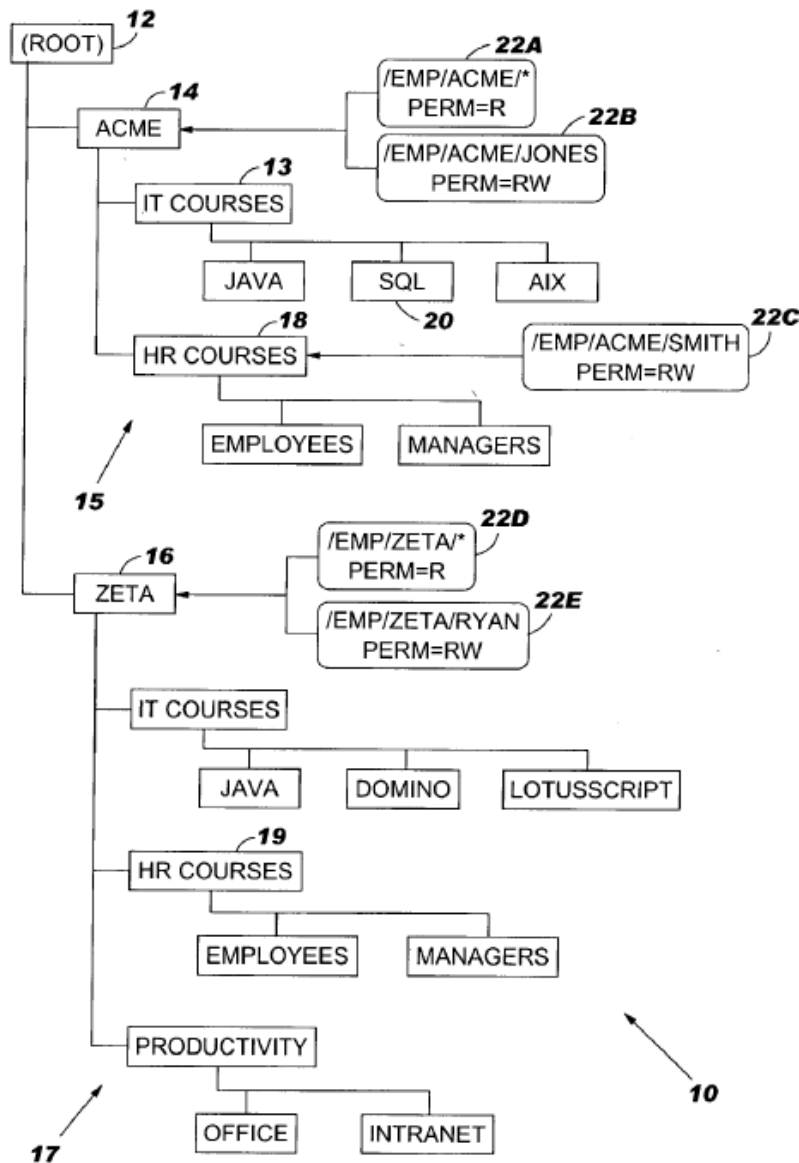


EX-1003 ¶148.

To the extent that Patent Owner argues Gladstone does not disclose or render obvious a *plurality of higher-level nodes* and *said base nodes arranged together... in the form of a tree hierarchy*, a POSA would have found this obvious in view of Salazar. EX-1003 ¶149. For example, Salazar discloses a typical

hierarchy of nodes included a “root node” that is the initial (or top) node of the hierarchy. The root node had one or more “child nodes” that were located at the level immediately below the root node, and the root node was called the “parent node of the child nodes”:

FIG. 1



EX-1009 [0020], FIG. 1. Salazar also states that “hierarchy of nodes 10 is **useful** in categorizing data items so that they can be **efficiently** located and retrieved.”

EX-1009 [0023]. Salazar further discloses that its method of associating its access

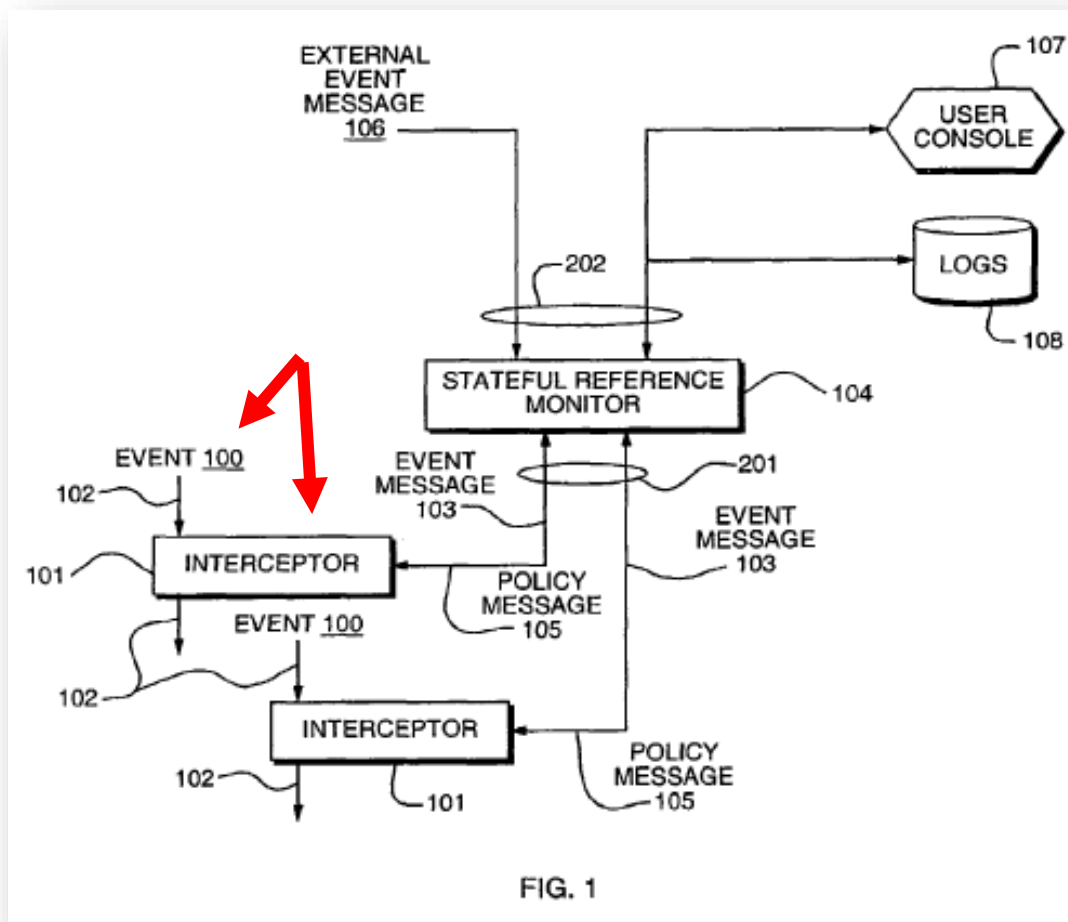
entries with the nodes “provides a more **flexible**, and **efficient** implementation of managing access to data items arranged into a hierarchy of nodes.” EX-1009 [0007]. A POSA would have recognized this efficiency as beneficial to the access control system and method described by Gladstone and, using this teaching, found it obvious to *arrange* Events X, Y and Z (*base nodes*) and their combination as X-Y-Z (*higher-level node*) *in the form of a tree hierarchy*. EX-1003 ¶149.

[10c] a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node;

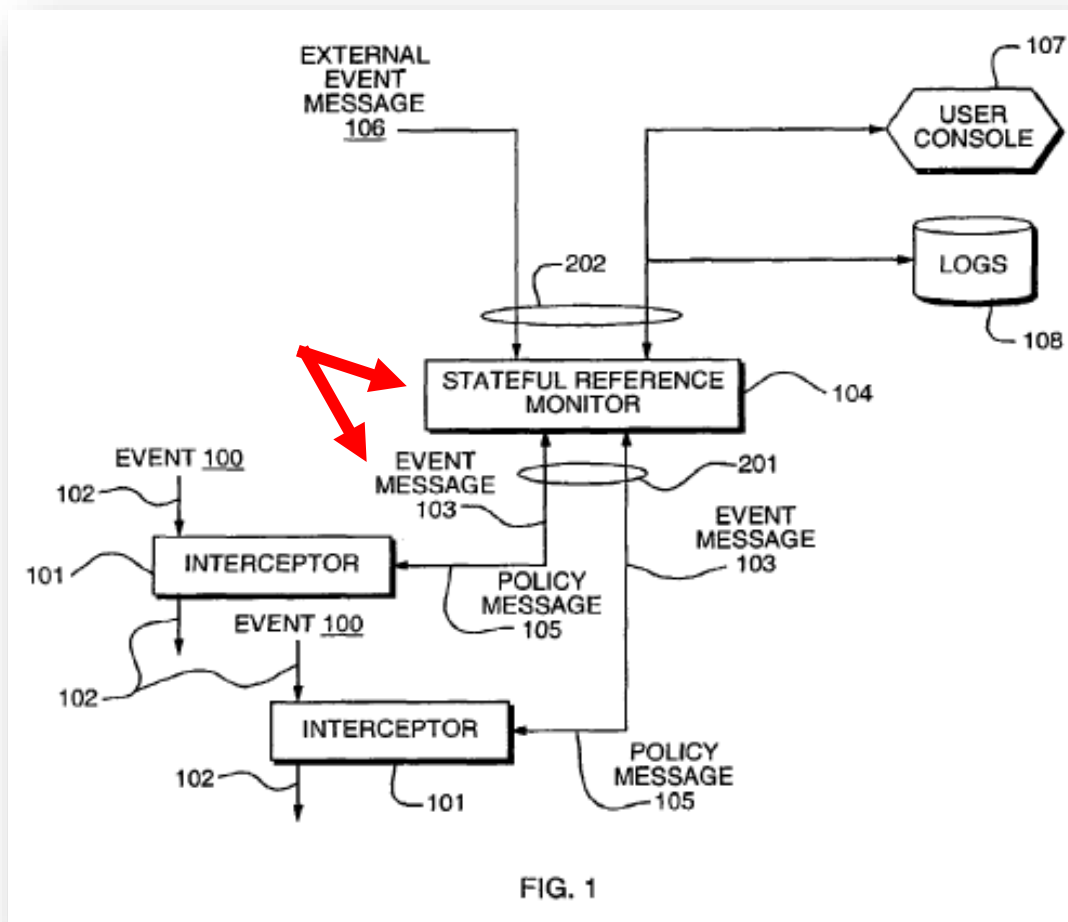
Gladstone discloses, or renders obvious alone or with Salazar, this limitation. EX-1003 ¶¶150-161.

Gladstone discloses a *plurality of logical base nodes* as described above in [10a]. *See* [10a]. Any one of these base nodes can be the *first base node*. EX-1003 ¶151.

Gladstone discloses intercepting (*receiving*) events 100 and event messages 103 (*a request... for access to a first base node*) by inceptor(s) 101 and stateless reference monitor and stateful reference monitor 104 of computer system 300 (*in said computer system*). For example, Gladstone discloses “[i]nterceptors 101” that “**intercept[]** various types of operating system **requests**, etc., **referred to herein as events**, for example requests for access to operating system resources such as a file or network connection”:



EX-1004 6:37-41, FIG. 1 (annotated); *see also* EX-1004 5:5-6-7 (“system **events 100**, e.g. **access requests** to a resource”). After “an event is intercepted by an interceptor 101,” it “generates an **event message 103**” that is “communicated to a **stateful reference monitor 104**” for stateful access control determinations:



EX-1004 5:16-24, 7:25-27, FIG. 1 (annotated). Both the intercepting of the event 100 by interceptor 101 and receiving the event message 103 by stateful reference monitor 104 are *receiving a request... for access*. EX-1003 ¶152.

Gladstone also discloses that its access control methods utilize “[c]onventional” “stateless reference monitors.” EX-1004 2:13-20. Gladstone discloses that “stateful reference monitor 104 acts as an **additional** processing step over and above any existing stateless reference monitor” and, “[t]hus, [the stateful reference monitor 104] cannot grant access when the standard stateless reference

monitor would have denied access.” EX-1004 10:48-52; EX-1003 ¶153.

Consequently, a POSA would have understood, or at least found obvious, that the request for access associated with interception of event 100 and event message 103 would also have been *received* by Gladstone’s integrated stateless reference monitor for its determination to allow or deny an access request prior to stateful reference monitor 104’s evaluation of that request. EX-1004 10:48-52; EX-1003 ¶153. Therefore, both of Gladstone’s stateless and stateful reference monitors *receiv[e the] request... for access*. EX-1003 ¶153.

As described above, interceptor 101, stateless reference monitor, and stateful reference monitor 104 each receive the request, are part of computer system 300, and are therefore each *a computer system interface* as claimed. Gladstone further discloses that application programming interface (API) 203 of monitor as another interface that receives the requests. EX-1004 5:44-48; EX-1003 ¶154.

Gladstone also discloses its requests are made by a user and user process (both, individually and combined, *an entity*). For example, Gladstone states that “reference monitor[s]”—such as its stateless reference monitors and stateful reference monitor 104—“determine[] whether an access by” “a user process” “is permitted.” EX-1004 1:64-67. These “[u]ser processes are” “identified to users on the basis of the user supplying certain identity tokens.” EX-1004 2:13-20.

Gladstone also states that access requests, *e.g.*, “events X, Y and Z” “may be”

“associated” “with the same user”—i.e., *entity*. EX-1004 6:21-24. Both the user and user process are *an entity* as described by the ’708 Patent. EX-1001 1:59 (“The entity can be a user or a process”); EX-1003 ¶155.

Gladstone’s user and user process (both, individually and combined, *an entity*) are, as modified by Salazar, each an entity with “user properties” (*with a predetermined access level*). For example, Gladstone describes its stateless reference monitors are “[c]onventional references monitors” “used to determine whether a particular **access** to a file or other resource is permitted.” EX-1004 2:1-12. In most cases, the stateless reference monitor’s “access decision is” “based on the **identity of the user**” “mak[ing] the request.” EX-1004 2:13-20. The access decision also references “permissions flags or an access control list associated with the resource,” “individual permissions [associated] with each user,” “a set of tokens” for “individual users,” and the “**rights** and **privileges** attributed to [a] **user**.” EX-1004 2:6-33, 8:2-3. Gladstone discloses that conventional “systems give finer control by associating individual permissions with each user.” EX-1004 2:30-33. Gladstone further discloses that the “conventional reference monitors” were “found in the kernels of various Operating Systems.” EX-1004 2:7-12. EX-1003 ¶156.

Salazar discloses that when a user requests data items and/or attempts to perform an operation on data items, access is allowed, or not, “based on one or

more particular user properties associated with user” (*a predetermined access level*) and, separately, “the access entries.” EX-1009 [0030-31]. Specifically, user properties are provided to an access system that separately obtains the access entries (*e.g.*, 22A-E) that then bases the access determination “on the one or more access entries that are **matched** with [the] user” using the property associated with the user (*a predetermined access level*) and the access entry. EX-1009 [0032-34]. EX-1003 ¶157.

Salazar discloses that these “user properties” broadly cover **any** property or characteristic that may be associated with a requesting user. For example, Salazar discloses that the “user property can be **any** property associated with a set of users such as a path/directory, a group designation, a user attribute, etc.” EX-1009 [0024]. This includes both a “group specific property or a **personal** property associated with [the] **user**.” EX-1009 [0029] (internal quotes omitted). User properties could further cover a user’s department, country, or role. EX-1009 [0034] (“Dept=ACME and Country=USA,” “isManager”); EX-1003 ¶158.

A POSA would have understood that Salazar’s broad disclosure of the “user property” that “can be **any** property” included the well-known and widely implemented security or classification levels (*i.e.*, *access levels*) used in prior art access control systems, which were known to implement access rules that “compar[ed]” a user’s “clearance/authorization,” “security level,” and/or

“hierarchical classification”—all examples of a *predetermined access level*—“to” the “[a]ccess control labels”—the “sensitivity level (e.g., classification)” or the *minimum access level*—“associated with objects” to determine whether to grant access. EX-1003 ¶159 (EX-1013 9-10, 60, 65, 111. EX-1014 [0032-37, 41], FIG. 1 (providing access control based on “sensitive,” “classified,” classifications of information and permissions of a user); EX-1007 Abstract, 2:5-9, 2:21-28, 4:23-26, 4:38-51 (“security rank” assigned to users that determined whether access to information would be allowed or denied, where, *e.g.*, “the top rank is A and the rank goes down one by one from A to Z”), FIG. 3:

FIG.3

430 USER ID TABLE		
431 USER ID	432 SECURITY RANK	433 ATTRIBUTE OF ANOTHER USER
C001	A	BELONGING, POSITION AND THE LIKE OF USER
C002	A	BELONGING, POSITION AND THE LIKE OF USER
C003	B	BELONGING, POSITION AND THE LIKE OF USER
C004	C	BELONGING, POSITION AND THE LIKE OF USER
C005	C	BELONGING, POSITION AND THE LIKE OF USER
B001	C	GUEST
B002	D	GUEST

EX-1016 017 (“[a]n **aggregate** of data might require a **higher classification** than the individual items”, EX-1001 1:24-27 (describing the “inevitabl[e]” and “natural[.]” understanding that aggregating information changes sensitivity levels)); §IV.F.1.

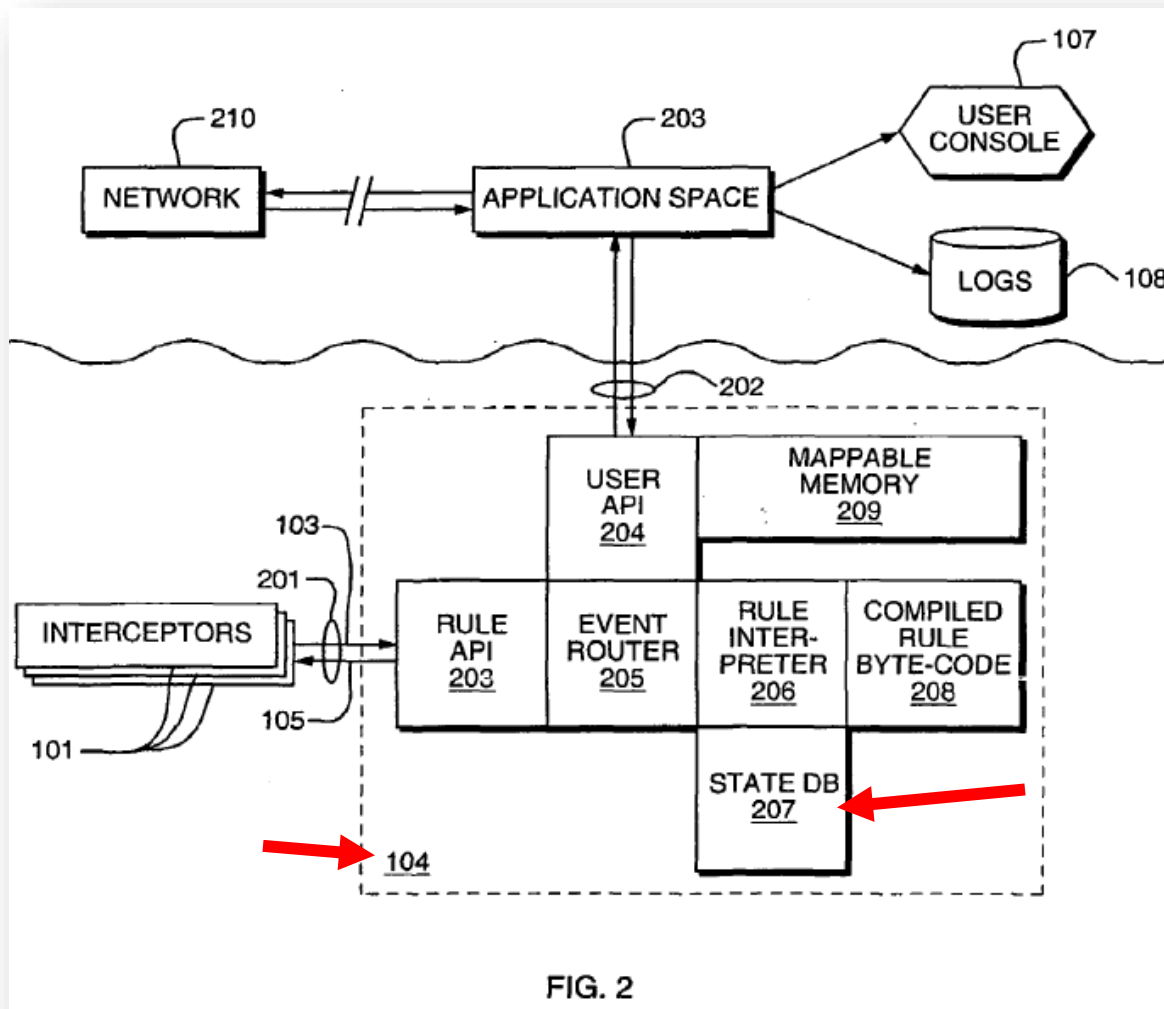
A POSA would have found it obvious to combine Salazar’s user properties (*a predetermined access level*) with Gladstone’s user and user process (both, individually and combined, *an entity*). EX-1003 ¶160. Both disclose access control decision systems that provide “fine control” by associating data with each user used in the access control decision. EX-1004 2:30-31; EX-1009 [0005]. Further, Salazar states that its fine control is enabled by managing access control at the “application level” (EX-1009 [0005])—the same level at which Gladstone’s stateful reference monitor 104 operates (EX-1004 6:24-33). A POSA would have recognized Salazar as describing the details of an example of a stateless reference monitor as described by Gladstone, and would have recognized that this fine-tuning of access control would benefit Gladstone’s system of implementing access control based on sequences of events at the user level, and thus motivated to make such modification. EX-1003 ¶160. A POSA would have had a reasonable expectation of success because comparative access-control systems where a “common security management” requiring nothing more than “simple relational

comparison,” as admitted by the ’708 Patent, was well within the skill of the POSA. EX-1003 ¶160 (EX-1007 4:37-44; EX-1001 1:25-28).

Finally, a POSA would have understood that Salazar’s user properties, including multi-level security ranks and/or classifications levels, would have been associated with Gladstone’s users prior to the access control decision and, therefore, are *predetermined*. EX-1003 ¶161. For example, Salazar states that its user properties 40 are “set[.]” “stored” and later “retriev[ed]” by various systems. EX-1009 [0029, 33]; EX-1003 ¶161.

[10d] a temporal access table;

Gladstone discloses a state database 207 (*a temporal access table*). EX-1003 ¶162. For example, Gladstone discloses that stateful reference monitor 104 contains a “state database 207 [that] is simply a repository of dynamic state information”:



EX-1004 5:58-67, FIG. 2 (annotated). “State information” is, “but is not limited to, information that a certain event occurred within a certain time of the present time.”

EX-1004 6:13-15. Gladstone provides an example of the recordation of these events (*i.e.*, requests for access to a resource) and the times at which they occur:

“Suppose a prohibited combination of events is denoted X-Y-Z. That is, Event X, Event Y and Event Z must occur within a certain timeframe to produce a bad result. Then, if the state database 207 holds information X-Y, a rule in byte-code

208 will prohibit Z. But, another rule in byte-code 208 will cause event X and/or event Y to be purged from state database 207 after a suitable time.” EX-1004 6:15-21; 8:5-13 (“information stored, may include some or all of, but not necessarily limited to, **time of the event, type of event, application generating the event, user owning the application and the like.**”). EX-1003 ¶162.

A POSA would have understood that Gladstone’s description and use of state database 207 to be the same as ’708 Patent’s description and use of a temporal access table. EX-1003 ¶163. First, a POSA would have understood a database, such as Gladstone’s state database 207, to be a table. EX-1003 ¶163. Second, Gladstone’s state database 207 is used in the same way as the ’708 Patent describes the Temporal Access Table shown in Figure 4B:

Temporal Access Table (TAT)							
Usr	A	B	C	D	dir	exec	del
1(1)					102	112	
2(1)							
3(2)					111	103	
4(1)							
5(3)							

EX-1001 FIG. 4B. Like Gladstone’s state database 207, the ’708 Patent’s Temporal Access Table maintains a history of the time at which operations performed. EX-1001 5:55-57. For example, as shown in Figure 4B (above), user 1 performs a “dir” operation at time “102” and then requested an “exec” operation at time “112.” EX-1001 5:62-66. A POSA would have understood that because the ’708 Patent’s Temporal Access Table is used in the same way as Gladstone’s state database 207, Gladstone discloses *a temporal access table*. EX-1003 ¶163.

[10e] processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level; and

Gladstone, in view of Salazar, renders obvious this limitation. EX-1003 ¶¶164-180.

Gladstone discloses *a processing means*. EX-1003 ¶165. For example, Gladstone discloses that its “invention relate[s] generally to software that controls an operating policy of a computer system”—such as general purpose computer system 300 having processor 303—to, *e.g.*, control “access to various system resources, such as files and network connections” by performing the functions below, as modified by Salazar where stated. EX-1004 1:22-25, 3:44-4:9 (“software product”), 14:20-57, FIG. 3. To the extent this limitation is governed by means-plus-function, Gladstone’s general purpose computer system 300

adapted by this software, as modified by Salazar where stated, to carry out algorithms performing the respective functions discussed below is the structure indicated in the '708 Patent or equivalent thereof (§IV.C) and, therefore, Gladstone, modified by Salazar where stated, discloses *a processing means* under any reasonable construction. EX-1003 ¶165.

As discussed above in [10c-d], Gladstone discloses events 100 and event messages 103 (both, individually and combined, *said access request*) and state database 207 (temporal access table) in the same manner as the '708 Patent. *See* [10c-d]; EX-1003 ¶166. As also discussed, Gladstone utilizes its state database 207 in the same manner as the temporal access table in the '708 Patent (*see* [10d]) and, therefore, likewise discloses *comparing said access request to said temporal access table*. EX-1003 ¶166.

To the extent that *comparing* requires the '708 Patent's temporal order table or equivalent structure (*see* §V.C.i), Gladstone discloses, or renders obvious, this same or equivalent structure. EX-1003 ¶167. For example, Gladstone discloses that it is “a rule in byte-code 208” that “prohibit[s] Z” “if the state database 207 holds information X-Y” EX-1004 6:18-19. Further, “various types of patterns of events can be programmed into the rules byte-code 208,” including rules generated in a “state collection mode, wherein normal combinations and patterns of activity are stored in state database 207.” EX-1004 9:11-27. A POSA would have

understood, or at least found obvious, that for the “various types of patterns of events” analyzed by Gladstone, the rules would be organized in the same form and format as the means by which those patterns were collected. EX-1003 ¶167. Specifically, such rules would be contained in a corresponding table of the “various types of patterns of events” because such rules were generated from just such a table—state database 207. *Id.*, *see* [10d]; EX-1003 ¶167. Further, a POSA would have understood that a table is the well-known options for organizing relational data (*e.g.*, related resource requests), and would have found it obvious to organize byte-code 208 as a table as a simple design choice. EX-1003 ¶167.

Gladstone discloses, or renders obvious alone or with Salazar, stateful reference monitor 104 using this comparison when *determin[ing] if*, for events 100 and event messages 103 (both, individually and combined, *said access request*), a sequence of actions should be denied (*completes a prohibited temporal access pattern*) for the user or user process (*for said entity*). EX-1003 ¶168.

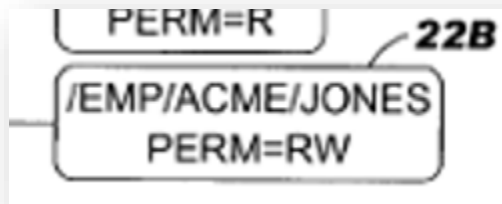
For example, Gladstone discloses that “various types of patterns of events can be programmed” “for detection and action” by the stateful reference monitor 104. EX-1004 9:11-27. Gladstone’s methods “track a **sequence of actions**” and can allow or deny requests. EX-1004 13:8-10. Such “sequences are used for detecting malicious behavior” and “normal behavior.” EX-1004 13:13-21. This functionality enables the “stateful reference monitor [to] ensure[] that requests are

ordered, i.e. **a request either happens before or after another request**”—i.e., that a *temporal access pattern* occurs or does not occur. EX-1004 12:22-28. For example, a “prohibited combination of events” of “X-Y-Z” would “prohibit Z” if the request for Event Z occurred while “state database 207 holds information X-Y”—indicating that events X and Y had already occurred. EX-1004 6:13-14; EX-1003 ¶169. While Gladstone discloses that event Z could be blocked based on the combination of events X-Y-Z, regardless of the order in which the events occurred, Gladstone also discloses “ensur[ing] that requests are **ordered**, i.e. a request either happens before or after another request” and “track[ing] a **sequence** of actions.” EX-1004 12:22-28; 13:8-10. Thus, a POSA would have understood that Gladstone discloses blocking (denying the request) combinations of actions due to the particular “sequence of actions” of those events and, therefore, would have found it obvious for the stateful reference monitor 104 to require a particular ordering of events X, Y, and Z for the security policy to be applied to them. EX-1003 ¶169. Therefore, a POSA would have found it obvious for Gladstone’s stateful monitor to deny access to event Z if a user requested access because the user had already requested access to event X and/or Y in a particular order. EX-1004 13:8-10, 12:22-28; EX-1003 ¶169. Gladstone expressly describes that monitoring the order of actions was the very purpose of stateful monitors—such as stateful reference monitor 104—that observed the “dynamic state” of computer systems using

information “collected in real-time, indicative of a condition of a machine or process as a result of a **particular sequence of events**.” EX-1004 2:1-4; EX-1003 ¶169. These disclosures of Gladstone also correspond to the ’708 Patent’s description of *temporal access patterns*: “**temporal ordering** of primitive access operations mandates that the operations occur **in the order specified** for the security policy to be enforced.” EX-1001 5:43-45. Therefore, Gladstone discloses *determining if said access request completes a prohibited temporal access pattern*, and applying its security policy based on the same. EX-1003 ¶169.

To extent that the *a prohibited temporal access pattern* requires the algorithm and structure comparing *access levels* (§V.C.i), this is obvious over Gladstone in view of Salazar. EX-1003 ¶170. As discussed above for [10c], Salazar discloses user properties, including “sensitivity level”—*a minimum access level*—to determine whether to grant access. *See* [10c]. A POSA would have found it obvious to combine Salazar’s user properties with Gladstone’s resources for the same reason as described with respect to the user or user processes. *See* [10c]; EX-1003 ¶170. For example, Salazar includes the user properties in the access entries. Salazar associates “access entries,” *e.g.*, access entries 22A-E, with various nodes of hierarchy 10 in Figure 1. EX-1009 [0024], FIG. 1. Each access entry 22A-E associates a “user property” with what Salazar describes as an “access level.” EX-1009 [0024]. For example access entry 22B associates the user

property “/EMP/ACME/JONES” with a “read/write” “access level” (i.e., “PERM=RW”):



EX-1009 [0027], FIG. 1; EX-1003 ¶170.

As described above in [10c], a POSA would have understood that Salazar’s broad disclosure of the “user property” that “can be any property” included the well-known and widely implemented security or classification levels (*i.e.*, access levels) used in prior art access control systems. *See* [10c]; EX-1003 ¶171.

A POSA would have found it obvious to use Salazar’s “user properties” in place of Gladstone’s one or more static permissions flags or as part of or in place of an access control list associated with the resource (as modified, *a minimum access level established for said first base node*) for the same reasons discussed above in [10c]. *See* [10c]; EX-1003 ¶172. Both disclose access control decision systems that provide “fine control” by associating data with each user used in the access control decision. EX-1004 2:30-31; EX-1009 [0005]. Further, Salazar states that its fine control is enabled by managing access control at the “application level” (EX-1009 [0005])—the same level at which Gladstone’s stateful reference

monitor 104 operates (EX-1004 6:24-33). A POSA would have recognized Salazar as describing the details of an example of a stateless reference monitor as described by Gladstone, and would have recognized that this fine-tuning of access control would benefit Gladstone's system of implementing access control based on sequences of events at the user level, and thus motivated to make such modification. EX-1003 ¶172. A POSA would have had a reasonable expectation of success because comparative access-control systems where a "common security management" requiring nothing more than "simple relational comparison," as admitted by the '708 Patent, was well within the skill of the POSA. EX-1003 ¶172. (EX-1007 4:37-44; EX-1001 1:25-28).

Further, a POSA would have understood, or at least found obvious, that Salazar's "user properties" for resources and access control decisions utilizing the same also applied to aggregated, combined resource requests, *e.g.*, the prohibited combination of events X-Y-Z. EX-1003 ¶173. This combination is an aggregation of events, which a POSA would have understood, or at least found obvious, to be subject to higher sensitivity or classification levels than the individual resources due to the aggregation or, nevertheless, subject to the sensitivity level of each individual resources request. EX-1003 ¶173 (EX-1016 017 ("[a]n **aggregate** of data might require a **higher classification** than the individual items"); EX-1001 1:24-27 (describing the "inevitabl[e]" and "natural[]" understanding that

aggregating information changes sensitivity levels)). A POSA would have been motivated to implement the “user properties” with an aggregation of events, *e.g.*, prohibited combined event X-Y-Z, for the same reasons provided above for the individual resources, and would have reasonably expected this combination to be successful as requiring nothing more than routine skill and a simple relational comparison. EX-1003 ¶173.

Therefore, Gladstone discloses, or renders obvious alone or with Salazar, *determining if said access request completes a prohibited temporal access pattern*, and applying its security policy based on the same. EX-1003 ¶174.

Gladstone also discloses that the blocked sequence of actions (*prohibited temporal access pattern*) is specific to a user and user process (*for said entity*). As discussed above for [10c], Gladstone discloses user and user process (both, individually and combined, *said entity*) having, as modified by Salazar’s user properties (*predetermined access level*) used in access determinations. *See* [10c]. Further, Gladstone states that the combination of “[e]vents X, Y and Z” “may be” “associated” “with the same user.”⁴ EX-1004 6:21-23. When the user or user

⁴ Gladstone also discloses that access control determinations based a sequence of events (*temporal access pattern*) could be made independent of the user (EX-1004 7:62-66), an embodiment not contemplated by the ’708 Patent, further illustrating

process (*said entity*) requests a particular sequence of events (e.g., events X-Y-Z) (*temporal access pattern*) that is blocked, a POSA would have understood that blocking to be directed at the user and, therefore, the blocked sequence of events is a *prohibited temporal access pattern* for the user or user process (*said entity*). EX-1003 ¶175.

To the extent that Gladstone does not expressly disclose blocking a sequence of events (*prohibited temporal access pattern*) specific to a particular user or user process (*for said entity*), a POSA would have nevertheless found doing so obvious. EX-1003 ¶176. Gladstone broadly discloses that “reference monitor[s]”—including stateful reference monitor 104—“determine whether an access by” “a user process” “is permitted.” EX-1004 1:64-67; 6:21-23; EX-1003 ¶176. These determinations “[i]n most cases” are “based on the identity of the user.” EX-1004 2:13-20. Gladstone describes that conventional security “systems give finer control by associating **individual permissions with each user.**” EX-1004 2:30-21. Thus, a POSA would have found it obvious to use both the “identity of the user” and the associated “individual permissions” in determining whether to block a sequence of events (*prohibited temporal access pattern*) for a particular user or

that the prior art had far surpassed the purported solutions that the ’708 Patent describes before the March 2004 priority date. EX-1003 ¶175 (§V.F.4); §IV.F.3.

user process (*for said entity*). EX-1003 ¶176 (EX-1010 2:63-3:1 (integrating user usage patterns in security rules); EX-1011 43-44 (determining consistency of “characteristic patterns of actions,” of users.)). A POSA would have been motivated to include this individualized access control capability in Gladstone’s stateful monitor 104 to achieve the same effect—provide access control based on the individual. EX-1003 ¶176. Further, a POSA would have had a reasonable expectation of success because, well before March 2004, “individual[ized] permissions” were already used by access control systems and that “operat[ing] on the basis of the user” “and the rights and privileges attributed to that user” was “conventional.” EX-1004 2:30-21, 7:66-8:3; EX-1003 ¶176 (§V.F.1); §IV.F.1. Therefore, Gladstone discloses or renders obvious *determin[ing] if said access request completes a prohibited temporal access pattern for said entity*. EX-1003 ¶176.

Gladstone, in view of Salazar, renders obvious making access control determinations by matching (*comparing*) the “user properties” of Gladstone’s resources (*a minimum access level established for said first base node*) to Salazar’s user properties associated with Gladstone’s user and user process (*said predetermined access level*). EX-1003 ¶177.

For example, Gladstone discloses that a “**reference monitor** is a component of a computer system that **determines** whether an access” “**is permitted.**” EX-

1004 1:64-67, 2:7-12. For example, Gladstone discloses that “[i]n most cases the access decision is made **based on** the identity of the user” “and one or more static permissions flags or an access control list associated with the resource” and matching in the context of access control lists. EX-1004 2:13-20, 2:30-33, 2:36-39. Likewise Salazar discloses that the access control decisions are “based on the one or more access entries that are **matched** with [the] user” using the property associated with the user and the access entry. EX-1009 [0032-34]. EX-1003 ¶178.

Gladstone, in view of Salazar, renders obvious implementing Salazar’s “user properties” with Gladstone’s resources (*a minimum access level established for said first base node*) for the reasons stated above. EX-1003 ¶179.

Therefore, Gladstone, in view of Salazar, renders obvious *comparing a minimum access level established for said first base node to said predetermined access level*. EX-1003 ¶180.

[10f] wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

Gladstone, in view of Salazar, renders these elements obvious. EX-1003 ¶¶181-185.

As discussed above, Gladstone, modified by Salazar where stated below, discloses or renders obvious processor 303, and a general purpose computer 300

adapted with an algorithm to perform the function discussed below, and, therefore, discloses *a processing means* having the same or equivalent structure indicated in the '708 Patent (§IV.C). *See* [10e]; EX-1003 ¶182.

As discussed above, Gladstone discloses that “stateful reference monitor 104 makes a decision” “to block or allow” a sequence of events (*prohibited temporal access pattern*) for the user or user process (*for said entity*). *See* [10e]. For example, Gladstone discloses that if “a prohibited combination of events is” “X-Y-Z,” stateful reference monitor 104 would “prohibit Z” if it had recorded in “state database 207” “[events] X-Y.” EX-1004 6:13-24; *see* [10e]. Conversely, a POSA would have understood that Gladstone’s monitor 104 would have allowed event Z if it did not complete a *prohibited temporal access pattern*, *e.g.*, if the combination of events X-Y-Z were allowed for the user, if the events occurred in some other order, if either of events X and Y had not been completed, or if the user had a sufficient clearance for the combination of events. EX-1003 ¶183. Therefore, Gladstone discloses or renders obvious *said processing means den[ying] said request if said access request completes a prohibited temporal access pattern for said entity and grant[ing] said access request only if it does not complete a prohibited temporal access pattern for said entity*. EX-1003 ¶183.

Gladstone, in view of Salazar, renders obvious *granting said access request only if ...* Salazar’s user properties associated with the Gladstone’s resource (*said*

minimum access level established for said first base node) also do not exceed the user property assigned to the user and/or user process (*said predetermined access level*). EX-1003 ¶184; *see also* [10c, 10e]. As discussed above, a POSA would have understood that Salazar’s “user property” included the well-known and widely implemented security or classification levels (*i.e., access level[s]*) used in prior art access control systems. *See* [10c, 10e]; EX-1003 ¶184 (EX-1013 9-10 (“what classes of information [users] are authorized to deal with” for “for handling sensitive (e.g., classified) information”); EX-1014 [0032-37, 41], FIG. 1 (providing access control based on “sensitive,” “classified,” classifications of information and permissions of a user); EX-1007 Abstract, 2:5-9, 2:21-28, 4:23-26, 4:38-51, FIG. 3 (disclosing a “security rank” assigned to users that determined whether access to information would be allowed or denied, where, *e.g.*, “the top rank is A and the rank goes down one by one from A to Z.”)); §IV.F.1. A POSA would have understood that requiring a “match” of user properties for (*see, e.g.,* EX-1004 1:38-2:44; EX-1009 [0026-27, 34-35]) would mean that *said minimum access level for said first base node* **does not exceed** *said predetermined access level* as “**does not exceed**” is used by the ’708 Patent. EX-1003 ¶184. EX-1001 3:36-41 (“The number represents a minimum security access level required for any process or user to access that particular function. Thus, for example, the “exec system function labeled exec(2) requires that a process or user possess a security level of

at least two in order to access that function.”). Further, a POSA would have understood that Gladstone in view of Salazar would allow access when the user property assigned to the user (*predetermined access level*) exceeded the user property assigned to the resource (*minimum access level for said first base node*). EX-1003 ¶184 (EX-1007 4:38-51 (disclosing a system where “the top rank is A and the rank goes down one by one from A to Z” and “if (the security rank of the user who wants to access the data)” is less than or equal to “(the security rank of the user whose data is to be accessed), the user who wants to access the data is” “permitted to access the data, while if not, he or she is not permitted to access.”)). Further, Gladstone expressly states that stateful reference monitor 104 “cannot grant access when the standard stateless reference monitor” “denie[s] access.” EX-1004 10:48-52. Thus, Gladstone in view of Salazar renders obvious *granting said access request only if ... said minimum access level for said first base node does not exceed said predetermined access level*. EX-1003 ¶184.

Therefore, Gladstone in view of Salazar renders obvious *wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level*. EX-1003 ¶185.

b. Claim 11

11. The secure computer system according to claim 10, wherein said processing means denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity.

Gladstone in view of Salazar renders obvious *the secure computer system according to claim 10*. See [10pre]-[10f]; EX-1003 ¶186.

As discussed above, Gladstone, alone or in view of Salazar, discloses or renders obvious processor 303, and a general purpose computer 300 adapted with an algorithm to perform the function discussed below, and, therefore, disclosing *a processing means* having the same or equivalent structure indicated in the '708 Patent (§IV.C). See [10e]; EX-1003 ¶187.

Gladstone also discloses *denying said request if said minimum access level for said first base node exceeds said predetermined access level for said entity* as discussed above. See Claim [10f]; EX-1003 ¶188.

c. Claim 12

12. The secure computer system according to claim 10 wherein said higher-level nodes are aggregations of said base nodes.

Gladstone in view of Salazar renders obvious *the secure computer system according to claim 10*. See [10pre]-[10f]; EX-1003 ¶189.

Gladstone discloses, or renders obvious, *wherein said prohibited combination of Events X-Y-Z (higher-level node[]) [is an] aggregation[] of said Event X, Event Y, and Event Z (base nodes)* as discussed above. See [10b]; EX-

1003 ¶190. As discussed above, a POSA would find it obvious to extend the teaching of Gladstone to multiple prohibited combinations of events as mere repetition of Gladstone's example. EX-1003 ¶190.

d. Claim 13

13. The secure computer system according to claim 12 wherein said processing means identifies within said hierarchy any higher-level nodes that are aggregations comprising said first base node.

Gladstone in view of Salazar renders obvious *the secure computer system according to claim 12*. See Claim 12; EX-1003 ¶191.

As discussed above, Gladstone, alone or in view of Salazar, discloses or renders obvious processor 303, and a general purpose computer 300 adapted with an algorithm to perform the function discussed below, and, therefore, disclosing *a processing means* having the same or equivalent structure indicated in the '708 Patent (§IV.C). See [10e]; EX-1003 ¶192.

Gladstone discloses *identif[ying] within said hierarchy any higher-level nodes that are aggregations comprising said first base node*. EX-1003 ¶194.

As explained above, the combination of Events X-Y-Z is a combination—or *aggregation*—and therefore a higher-level node, of Events X, Y and Z, any of which may be the *first base node*; and, these higher-level and base nodes are arranged in a *hierarchy*. See [10b]; EX-1003 ¶194. Gladstone also discloses that stateful monitor 104 is aware of a prohibited combination of X-Y-Z, records the

occurrence of any of the events X, Y and Z, and blocks the last event of the combination, e.g., event Z, when the other two have been performed. EX-1004 6:13-19. A POSA would have understood that, in performing the above, stateful reference monitor 104 is identifying the *aggregated* node associated with prohibited combination of events X-Y-Z when, e.g., the first base node associated with, e.g., event Z is blocked. EX-1003 ¶194. Therefore, Gladstone discloses, or at least renders obvious *identif[ying] within said hierarchy any higher-level nodes that are aggregations comprising said first base node*. EX-1003 ¶194.

e. Claim 14

14. The secure computer system according to claim 13 wherein said computer processing means identifies within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.

Gladstone in view of Salazar renders obvious *the secure computer system according to claim 13*. See Claim 13; EX-1003 ¶195.

As discussed above, Gladstone, alone or in view of Salazar, discloses or renders obvious processor 303, and a general purpose computer 300 adapted with an algorithm to perform the function discussed below, and, therefore, disclosing *a processing means* having the same or equivalent structure indicated in the '708 Patent (§IV.C). See [10e]; EX-1003 ¶196.

Gladstone discloses, or renders obvious alone or in combination with Salazar *identif[ying] within said hierarchy any nodes that comprise children of any*

generation of said higher-level nodes that are aggregations comprising said first base node as discussed above. As explained above, Gladstone discloses that stateful monitor 104 is aware of a prohibited combination of X-Y-Z, records the occurrence of any of the Events X, Y and Z, and blocks the last event of the combination, *e.g.*, Event Z, when the other two have been performed. EX-1004 6:13-19. A POSA would have understood that blocking Event Z and the recognition of the occurrence of Events X and Y is *identif[ying] within said hierarchy* Events X, Y, and Z (*any nodes that comprise children of any generation*) of prohibited combination of X-Y-Z (*said higher-level nodes that are aggregations comprising said first base node.*). See [10e]; EX-1003 ¶197.

VII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION

A. The Board Should Not Deny Institution Under 35 U.S.C. § 325(d)

Denial under § 325(d) is not warranted because the challenges presented in this Petition are neither cumulative nor redundant to the prosecution of the '708 Patent. None of the asserted prior art references were cited or considered by the Examiner during prosecution of the '708 Patent, thus the references in this Petition were neither relied upon during prosecution nor are cumulative of art relied upon during prosecution. See EX-1002.

Petitioner has concurrently filed a Motion for Joinder seeking joinder with the *inter partes* review in Cisco Systems, Inc. v. Lionra Technologies Ltd, IPR2023-

00670 which also challenged Claims 10-14 of the '708 Patent ("the -0670 IPR"). Separately, and concurrently herewith, Petitioner is filing another Petition and corresponding Motion for Joinder seeking joinder with the *inter partes* review in Cisco Systems, Inc. v. Lionra Technologies Ltd, IPR2023-00669 which challenged Claims 1-6 and 9 of the '708 Patent ("the -0669 IPRs"). Other than the -0669 and -0670 IPRs, the '708 Patent has not been challenged in any other IPR or post-grant review (PGR) proceeding or in reexamination. The combination of art in the present grounds, and the arguments related thereto were not previously presented to the Office.

B. The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)

The Board has discretion to deny *inter partes* review under 35 U.S.C. § 314(a). In *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (Mar. 20, 2020) (precedential), the Board set forth six non-dispositive factors intended to guide that discretionary decision of whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding. On June 21, 2022, the Director issued interim procedure regarding application of the *Fintiv* factors ("Interim Procedure").

As set forth in the Board's decision in the -0670 IPR, the Board's decision is guided by analysis under *Fintiv* is guided by the USPTO Director's Memorandum issued on June 21, 2022, titled "Interim Procedure for Discretionary Denials in AIA

Post Grant Proceedings with Parallel District Court Litigation” (“Director’s Memo”). Pursuant to the Director’s Memo, the Board “will not discretionarily deny institution . . . where a petitioner presents a [*Sotera*] stipulation.” Director’s Memo at 3 (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (precedential as to § II.A)). Petitioner hereby stipulates that if the present proceeding is instituted and joined with the -0670 IPR, it will “not pursue in the co-pending district court litigation the specific ground asserted in the petition, or any other ground that was raised or could have been reasonably raised in an IPR (i.e., grounds that could have been raised under §§ 102 or 103 on the basis of prior art patent or printed publications).”

The Interim Guidance also stated that “the PTAB will not deny institution of an IPR or PGR under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” Here, the Petition presents compelling evidence of unpatentability of the Challenged Claims. Specifically, the Petition explains how the primary reference, Gladstone, discloses the claimed “temporal access pattern”—the only possible feature not in the art as admitted by the Applicant during prosecution and in the ’708 Patent specification—in the same manner described by the ’708 Patent. (§§IV.A-B, VI.A.4). Additionally, Gladstone, in combination with other references, renders obvious all remaining limitations of the Challenged Claims. Furthermore, in the -0670 IPR, the Board found that Cisco had established a reasonable likelihood

of success in showing that Claims 10-14 would have been obvious in view of the references and grounds cited in the current Petition. -0670 IPR, Paper 10 at 62.

Thus, under the Interim Procedure, the Board should not deny institution.

Nevertheless, a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).

Under factor 2, the trial date has been set for all defendants in the Related Litigation for May 2024. According to the most recent statistics on median time-to-trial for civil actions in E.D. Texas (EX-1019 035), the median time from filing to trial is 21 months. The Related Litigation was filed on August 8, 2022 and thus would be expected to go to trial shortly after May 8, 2024 according to the median time to trial statistics. A Final Written Decision in the -0670 IPR is expected in August 2024. Considering the inherent uncertainties of litigation scheduling, particularly where multiple trials are scheduled for the same date this factor weighs against discretionary denial.

Factor 3 is neutral in light of the motion for joinder.

Under factor 4, Petitioner has provided a *Sotera* stipulation.

Under factor 5, Petitioner is a defendant in the Related Litigation.

Under factor 6, other circumstances weigh in favor of institution as discussed above.

VIII. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Party-in-Interest (37 C.F.R. §42.8(b)(1))

Petitioner certifies that Petitioner Fortinet, Inc. is the real party-in-interest.

B. Related Matters (37 C.F.R. §42.8(b)(2))

1. Judicial Matters

As of the filing date of this Petition and to the best knowledge of Petitioner, the '708 Patent has been involved in the following litigation(s):

Lionra Technologies Limited v. Fortinet, Inc., E.D. Tex. Case No. 2:22-cv-00322 (filed Aug. 19, 2022) (ongoing).

Lionra Technologies Limited v. Cisco Systems, Inc., E.D. Tex. Case No. 2:22-cv-00305 (filed Aug. 8, 2022) (ongoing).

Lionra Technologies Limited v. VMware, Inc., W.D. Tex. Case No. 1:23-cv-929 (filed August 7, 2023) (ongoing).

2. Administrative Matters

As of the filing date of this Petition and to the best knowledge of Petitioner, the '708 Patent is subject to the following *inter partes* reviews.

IPR2023-00670.

IPR2023-00669.

The grounds presented herein are identical to the grounds presented in IPR2023-00670, and Petitioner files concurrently with this Petition a Motion for Joinder.

Additionally, Petitioner has filed a second petition challenging Claims 1-6 and 9 of the '708 Patent. Otherwise, as of the filing date of this Petition and to the best knowledge of Petitioner, the '708 Patent has not been the subject of any other *inter partes* reviews, reissues, or reexaminations.

C. Lead/Back-up Counsel (37 C.F.R. §42.8(b)(3))

Lead Counsel:

Monté T. Squire, USPTO Reg. 80,123
DUANE MORRIS LLP, 1201 North Market Street, Suite 501
Wilmington, DE 19801
P: (302) 657-4918; F: (302) 397-2543; MTSquire@duanemorris.com

Back-Up Counsel:

Patrick McPherson, USPTO Reg. 46,255
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-5214; F: (202) 776-7801; PDMcPherson@duanemorris.com

Paul H. Belnap, USPTO Reg. 73,106
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-7879; F: (202) 776-7801; PHBelnap@duanemorris.com

Patrick C. Muldoon, Reg. No. 47,343
PCMuldoon@duanemorris.com

DUANE MORRIS LLP
901 New York Avenue NW, Suite 700-East

Washington, D.C. 20001 P: 202.776.7840, F: 202.776.7801
--

D. Notice of Service Information (37 C.F.R. §42.8(b)(4))

Please direct all correspondence to lead and back-up counsel at the above addresses. Petitioner consents to electronic service at the email addresses above.

IX. CONCLUSION

For the reasons set forth above, Petitioner has shown a reasonable likelihood of prevailing on all Challenged Claims of the '708 Patent and requests that the Board institute *inter partes* review and cancel all claims as unpatentable.

Dated: November 14, 2023

Respectfully submitted,

DUANE MORRIS LLP

BY: /Monté T. Squire/

Monté T. Squire, USPTO Reg. 80,123

DUANE MORRIS LLP

1201 North Market Street, Suite 501

Wilmington, DE 19801

ATTORNEY FOR PETITIONER

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on November 14, 2023, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent 7,302,708 and all supporting exhibits were served via Federal Express, postage prepaid, to the correspondence address of record for the '708 Patent:

L3Harris Technologies, Inc.
C/O FOX ROTHSCHILD, LLP
997 Lenox Drive
Building 3
Lawrenceville, NJ 08543-5231
UNITED STATES

Dated: November 14, 2023

Respectfully submitted,

DUANE MORRIS LLP

BY: /Monté T. Squire/
Monté T. Squire, USPTO Reg. 80,123
DUANE MORRIS LLP
1201 North Market Street, Suite 501
Wilmington, DE 19801

ATTORNEY FOR PETITIONER

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. §42.24 *et seq.*, the undersigned certifies that this document complies with the type-volume limitations. This document contains 13,980 words as calculated by the “Word Count” feature of Microsoft Word 2016, the word processing program used to create it.

Dated: November 14, 2023

Respectfully submitted,

DUANE MORRIS LLP

BY: /Monté T. Squire/

Monté T. Squire, USPTO Reg. 80,123

DUANE MORRIS LLP

1201 North Market Street, Suite 501

Wilmington, DE 19801

ATTORNEY FOR PETITIONER