TC2400 - Search Workshop 2.0

Chirag Shah - TCOM TC 2400
Luu Pham - SPE AU 2439
Search Workshop 2.0 - Overview

- **Software Partnership**
  - Roundtable - Dec 2013
  - Federal Reg. Notice - Jan 2014
  - Recommendations based on roundtable and Federal Reg. Notice comments
    - Search recordation
    - Additional training on best practices
    - Education on search resources

- **Execution of Search Workshop Pilot 1.0 – FY 2016 Q1-Q2**
- **Evaluation and Case Study of Search Workshop Pilot 1.0 – FY 2017**
  - Increase trend in clarity of rejections made based on MRF Review
  - Increase trend in awareness of STIC/NPL database resources for search availability

- **Phase 1: Search Workshop 2.0: FY 2018-FY 2019**
- **Phase 2: Search 2.0 Trainings on three Tracks: FY 2020**
- **Phase 3: Expansion Considerations: FY 2021**
Training Milestones

Phase 1
FY19 – Q3

- Delivered Search 2.0 Hand-on workshop to ~500 Examiners in 7 AUs in each TC (TC 2100, 2400, 2600, 2800 and 3700)

Phase 2
FY20 – Q3-Q4

- Delivered three training sessions on three tracks (i.e., keywords, CPC, NPL) to ~500 examiners in 7 AUs in each TC (TC 2100, 2400, 2600, 2800 and 3700)

Phase 3
On-going

- Expansion to 22 AUs in TC2100 for CPC track, to 9 AUs in TC2400 for all 3 tracks, and to all WGs in TC2800
- Expansion Considerations to other TCs and Workgroups
Search Workshop 2.0 –
Phase 2: Training Objectives

• Increase likelihood of finding relevant prior art by applying a search loop framework to a Technology-focused example

• Develop and refine search concepts for Keyword, CPC and NPL tracks (by reviewing documents) and iteratively adjusting subsequent search queries

• Help examiners recognize and resolve potential issues among search queries by presenting effective techniques to monitor and adjust search queries
Search Workshop 2.0 – Methodology

- **What:** Interactive search training with animations
- **Who:** Participants: ~35 AUs across five Technology Centers (TC2100, TC2400, TC2600, TC2800 and TC3700)
- **Where:** Online WebEx platform
- **When:** FY20 and FY21 (expansion consideration)
- **Team/Resources:** TC Directors, TC POCs, PM, TC SPEs, Subject mater experts (primary examiners), STIC Searchers, OPQAs (RQAS), OPLA and PTA
Search 2.0 Characteristics

- Progression of Search
- Visually demonstrating the progression of Search
- Search Loop Framework
- Post-search Self-assessment
Progression of Search

Ways to narrow
- Add concepts
- Narrow concepts
- Change operators
  \( \text{AND} \rightarrow \text{SAME/WITH} \)
- Limit by CPC
  Groups/Subgroups
- Exclude concepts
  Use NOT
- Reorganize concepts
- Limit by Date
- Many other options possible
Visually Demonstrating Search Progression

Prior Art

Multi Ch. Auth. CPC

Indices

(S1 AND S2) AND (((multi$4 ADJ channel)(two ADJ channel)(second ADJ channel)(out$1of$1band)(out ADJ4 band)(OOB$1)) NEAR6 (authenticat$4 authoriz$5 log$4in$1)).ab,ti,bsum.

S3

Limit by Searchable Indices

S2

S1 AND (H04L9/32$ H04L63/08$ G06F21/30-40 H04W12/06).CPC

Limit by CPC

S1 (((multi$4 ADJ channel)(two ADJ channel)(second ADJ channel)(out$1of$1band)(out ADJ4 band)(OOB$1)) NEAR6 (authenticat$4 authoriz$5 log$4in$1))

Inventive Concepts

References

Hits: 692 Relevant: At least 21

Hits: 1866 Relevant: At least 29

Hits: 3934 Relevant: At least 34
Iterative Search loop

Understand invention
Develop collection of terms
Plan and execute your search
Perform preliminary search activities
## Applying Search Framework

### Case Study: Analyze Relevant References vs “Hits”

By color-coordinating different searches, participants can visually see the effects of limiting searches.

- As denoted by the “X”, participants see which queries eliminate relevant reference while reducing the number of “Hits”

### Hits: Size of the “haystack”

### Relevant references: Number of relevant documents within the “haystack”

### Table: Search Framework Analysis

<table>
<thead>
<tr>
<th>L#</th>
<th>Hits</th>
<th>Relevant references within hits</th>
<th>Excluded references</th>
<th>Potential 102 references remaining (from 14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L7</td>
<td>2501</td>
<td>23</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>L8</td>
<td>488</td>
<td>19</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>L4</td>
<td>509</td>
<td>15</td>
<td>12</td>
<td>9</td>
</tr>
<tr>
<td>L9</td>
<td>153</td>
<td>13</td>
<td>14</td>
<td>8</td>
</tr>
</tbody>
</table>

### Diagram: Schematic Representation

- L9: L7 AND L4
- L4: (detect$4 \text{ or } sens$4 \text{ or } infrared \text{ or } (pressure NEAR3 sens$4) \text{ or } micro$switch \text{ or } (conduct$4 \text{ NEAR3 sens$4} \text{ or } photo$optical \text{ or } ultrasonic \text{ or } electro$d$4) \text{ SAME L3}
Self-assessment tool

Conducting your search

Using CPC - Classification searches

1. Indicate your degree of confidence that you used the appropriate CPC symbols

<table>
<thead>
<tr>
<th></th>
<th>Extremely confident</th>
<th>Very confident</th>
<th>Not Very confident</th>
<th>Total lack of confidence</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

If Total lack of confidence: Why? What would improve your confidence?

________________________________________________________________________

________________________________________________________________________

2. I found my CPC symbols using the following tools:

- [ ] CPC QN
- [ ] CAT tool (Classification Allocation Tool) (Google Chrome only)
- [ ] CPC Crosswalk
- [ ] EAST Classification Robust Query Builder
- [ ] Prior of record (e.g., International Search Report)
- [ ] Other: ________________________________
Self-assessment tool

3. Indicate your degree of confidence that your CPC queries have included ranges to include the corresponding child (indent) symbols (Example: When CAT tool suggests G06F 17/30292, the EAST query is: G06F17/30292-30297.cpc.)

<table>
<thead>
<tr>
<th>Extremely confident</th>
<th>Very confident</th>
<th>Not Very confident</th>
<th>Total lack of confidence</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Using Keywords – Text Searching

4. Indicate your degree of confidence that you used the appropriate keywords

<table>
<thead>
<tr>
<th>Extremely confident</th>
<th>Very confident</th>
<th>Not Very confident</th>
<th>Total lack of confidence</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

If Total lack of confidence: Why? What would improve your confidence?
Surveys and Evaluations

• Participant Surveys (4 total)
  – Phase 1: After the Initial Workshop 2.0 training
  – Phase 2: After each of the 3 unique tracks for:
    • Keywords,
    • CPC, and
    • NPL

• Phase 2: OPQA Search Evaluations (2 total)
  – “Before” the Initial workshop 2.0 training, and
  – “After” the completion of the 3 tracks
Survey Data – Phase 1 Workshop

Overall, how satisfied were you with Search Workshop 2.0?
From 290 Total Responses

- Very dissatisfied: 3.8%
- Somewhat dissatisfied: 2.8%
- Neither dissatisfied nor satisfied: 8.3%
- Somewhat satisfied: 37.2%
- Very satisfied: 47.9%
Phase 2: Three Training Tracks

Technology Specific Example for Three Training Tracks

- **Keyword Track**
  
  Articulate search terms and conduct search based on keywords using internal EAST search tool

- **Classification Track**
  
  Articulate search terms and conduct search based on CPC classification using internal EAST search tool

- **NPL Track**
  
  Articulate search terms and conduct search utilizing NPL Search Engines (i.e., IP.com, GoogleScholar, IEEE, etc.;)
Survey Data – Technology specific Tracks

Overall, were you satisfied with the training?

- Keywords: 97% Yes, 3% No
- CPC: 96% Yes, 4% No
- NPL: 95% Yes, 5% No
Survey Data – Technology specific Tracks

Q7. 5 The graphics and animations in the course helped me understand course content..

- **Keywords**
  - Strongly Disagree: 3%
  - Disagree: 3%
  - Agree: 34%
  - Strongly Agree: 60%

- **CPC**
  - Strongly Disagree: 3%
  - Disagree: 3%
  - Agree: 40%
  - Strongly Agree: 54%

- **NPL**
  - Strongly Disagree: 3%
  - Disagree: 3%
  - Agree: 51%
  - Strongly Agree: 43%
Survey Data – Technology specific Tracks

Q7. 6 I plan to apply the knowledge and skills learned in this course.

- **Keywords**
  - Strongly Disagree: 3%
  - Disagree: 34%
  - Agree: 59%
  - Strongly Agree: 3%

- **CPC**
  - Strongly Disagree: 3%
  - Disagree: 39%
  - Agree: 55%
  - Strongly Agree: 3%

- **NPL**
  - Strongly Disagree: 2%
  - Disagree: 49%
  - Agree: 47%
  - Strongly Agree: 3%

TC 2400 - Prior Art Search 2.0
Survey - Takeaways

• Phase 2: Search Workshop had satisfaction scores ranging from 95-97%
• 93-96% agreed/strongly agreed that “I plan to apply the knowledge and skills learned in this course” for the technology-specific tracks (Keywords, CPC, and NPL)
• The Phase 2 (keyword, CPC, and NPL) technology-specific tracks performed better than the Phase 1
Search Evaluations

• “Before” and “After” reviews:
  – “Before” reviews were sampled prior to the initial Search Workshop 2.0 session (May 2019)
  – “After” reviews were sampled after the completion of the 3 tracks (August 2020)

• Evaluated Examiner’s search strategy and results form (e.g., EAST Search History queries)

• Reviewed Search information (e.g., Documented NPL databases)
Phase 2: Evaluation Takeaways

• NPL documentation on SRFW increased to 43% (+12 percentage points) where at least one NPL source cited
• Increased use of appropriate CPC symbols (+6 percentage points)
• Increased of combining CPC with Keywords (+12 percentage points)
• Searches used more synonyms
• In general, the searches reflected more iterative search behaviors due to:
  – Fewer Home-Run searches
  – Fewer prematurely abandoned search paths
  – Fewer restrictive keywords and CPC symbols
Search 2.0 - Keyword Track
TC 2400 – User Authentication Example
Understand the Invention

[0006] The invention is directed to a system and method for securely authenticating user using multi-channel authentication.

[0007] In one aspect of the present invention, a user 100, who has already created a valid account and registered his/her mobile device 103 to the server 102, is able to access to network resources after successfully authenticating in both in-band and out-of-band authentications.

[0008] User 100, may access to a web browser and sends a login request to a server using in-band communication channel between the user device 101 and server 102. The server 102 performs an initial authentication to authenticate user 100 using user’s credential (i.e., username and password) including in the login request. Server 102 validates user’s credential; if user’s credential is valid, the server will generates an authentication code (e.g., one-time passcode (OTP)) and sends the authentication code to the mobile device 103 via an out-of-band channel. User 100 enters the authentication code into a verification webpage displayed on the user device 101 and submits the authentication code to the server 102 for authentication. After receiving the authentication code from user device 101, server 102 will validate the authentication code. User 100 will be granted access to network resource if the received code/OTP matches with the code/OTP sent to the mobile device.
The invention is directed to a system and method for securely authenticating a user using multi-channel authentication.

In one aspect of the present invention, a user 100, who has already created a valid account and registered his/her mobile device 103 to the server 102, is able to access network resources after successfully authenticating in both in-band and out-of-band authentications.

User 100 may access to a web browser and sends a login request to a server using in-band communication channel between the user device 101 and server 102. The server 102 performs an initial authentication to authenticate user 100 using user's credential (i.e., username and password) included in the login request. Server 102 validates user's credential; if user's credential is valid, the server will generates an authentication code (e.g., one-time passcode (OTP)) and sends the authentication code to the mobile device 103 via an out-of-band channel. User 100 enters the authentication code into a verification webpage displayed on the user device 101 and submits the authentication code to the server 102 for authentication. After receiving the authentication code from user device 101, server 102 will validate the authentication code. User 100 will be granted access to network resource if the received code/OTP matches with the code/OTP sent to the mobile device.

Understand the Invention

1: User 100 sends a login request including username password to server 102 using device 101
2: Server 102 validates user's credential;
3. If user credential is valid, server 102 generates and sends an OTP to a registered mobile device 103;
4. User sends the OTP, using the first device 101, to server 102 for authentication.
5: Match OTP Authenticate User

TC 2400 - Prior Art Search 2.0 24
The invention is directed to a system and method for securely authenticating a user using multi-channel authentication.

In one aspect of the present invention, a user 100, who has already created a valid account and registered his/her mobile device 103 to the server 102, is able to access network resources after successfully authenticating in both in-band and out-of-band authentications.

User 100 may access to a web browser and sends a login request to a server using in-band communication channel between the user device 101 and server 102. The server 102 performs an initial authentication to authenticate user 100 using user’s credential (i.e., username and password) including in the login request. Server 102 validates user’s credential; if user’s credential is valid, the server will generate an authentication code (e.g., one-time passcode (OTP)) and sends the authentication code to the mobile device 103 via an out-of-band channel. User 100 enters the authentication code into a verification webpage displayed on the user device 101 and submits the authentication code to the server 102 for authentication. After receiving the authentication code from user device 101, server 102 will validate the authentication code. User 100 will be granted access to network resource if the received code/OTP matches with the code/OTP sent to the mobile device.

Understand the Invention

Claim 1: A method for authenticating a user using multi-channel authentication, the method comprising:

- receiving a login request from a first device,
  the login request includes user’s credential;

- in response to a verification that user’s credential is valid,
  generating an authentication token; and
  sending the authentication token to a registered mobile device;

- receiving a response from the user; and

- authenticating the user based on the received response.
Understand the Invention

- Understand invention
- Plan and execute your search
- Develop collection of terms
- Perform preliminary search activities
Claim 1: A method for authenticating a user using multi-channel authentication, the method comprising:

receiving a login request from a first device, the login request includes user’s credential;

in response to a verification that user’s credential is valid, generating an authentication token; and

sending the authentication token to a registered mobile device;

receiving a response from the user; and

authenticating the user based on the received response.
Understand the Invention

Reading Claims – Understanding Claimed Limitations

Claim 1: A method for authenticating a user using multi-channel authentication, the method comprising:

What is “multi-channel authentication”?

What is “authentication token”?

What is “registered mobile device”?
Claim 1: A method for authenticating a user using multi-channel authentication, the method comprising:

- receiving a login request from a first device, the login request includes user’s credential;
- in response to a verification that user’s credential is valid, generating an authentication token; and
- sending the authentication token to a registered mobile device;
- receiving a response from the user; and
- authenticating the user based on the received response.

Let’s draw a claim diagram

Determine if the claim fully describes the invention!

Note: Most of the time, independent claims are broad, dependent claims may recite limitations that better describe the invention.
Claim 1: A method for authenticating a user using multi-channel authentication, the method comprising:

1: Receiving a login request from a first device, the login request includes user's credential;

2: Validating if user's credential is valid;

3: Generating an authentication token;

4: Sending the authentication token to a registered mobile device;

5: In response to a verification that user's credential is valid, authenticate the user based on the received response.
1: User 100 sends a login request including username password to server 102 using device 101
2: Server 102 validates user’s credential;
3. If user credential is valid, server 102 generates and sends an OTP to a mobile device 103;
4. User sends the OTP, using device 101, to server 102 for authentication.
Understand the Invention
Reading Specs

[0006] The invention is directed to a system and method for securely authenticating user using multi-channel authentication.

[0007] In one aspect of the present invention, a user 100, who has already created a valid account and registered his/her mobile device 103 to the server 102, is able to access to network resources after successfully authenticating in both in-band and out-of-band authentications.

[0008] User 100, may access to a web browser and sends a login request to a server using in-band communication channel between the user device 101 and server 102. The server 102 performs an initial authentication to authenticate user 100 using user’s credential (i.e., username and password) including in the login request. Server 102 validates user’s credential; if user’s credential is valid, the server generates an authentication code, which is a one-time passcode (OTP), and sends the authentication code to the mobile device 103 via an out-of-band channel. User 100 enters the authentication code into a verification webpage displayed on the user device 101 and submits the authentication code to the server 102 for authentication. After receiving the authentication code from user device 101, server 102 will validate the authentication code. User 100 will be granted access to network resource if the received authentication code matches with the authentication code sent to the mobile device.
Develop
Collection of Terms

Understand invention
Develop collection of terms
Plan and execute your search
Perform preliminary search activities
Understanding Claimed Limitations
How spec defines the claimed limitations

Claim 1: A method for enhancing user’s authentication using multi-channel authentication, the method comprising:

- receiving a request, from a user via a first device, for access to network resources, the request includes user’s credential;
- in response to a verification that user’s credential is valid, generating an authentication token; and
- sending the authentication token to a registered mobile device;
- receiving a response from the user; and
- authenticating the user based on the received response.

What is “multi-channel authentication”?
Authenticate using two channel communications
- In-band auth.
- Out-of-band auth.

What is “authentication token”?
OTP, code, etc.,

What is “registered mobile device”?
Mobile device registered and associated with user’s account.
Claim 1: A method for authenticating a user using multi-channel authentication, the method comprising:

- receiving a login request from a first device, the login request includes user’s credential;
- in response to a verification that user’s credential is valid, generating an authentication token, and
- sending the authentication token to a registered mobile device;
- receiving a response from the user; and
- authenticating the user based on the received response.
Perform Preliminary Search Activities

- Understand invention
- Develop collection of terms
- Plan and execute your search
- Perform preliminary search activities
Perform Preliminary Search Activities

- Inventor name/assignee search in EAST/WEST/PALM
- Review related documents
  - Family applications
  - Foreign search reports (i.e., PCT search reports, Global Dossier),
  - IDS, etc.,
- Identify CPC symbols – class/subclass – group/subgroup
Perform Preliminary Search Activities

Identify Corresponding CPC Class/Subclass

View corresponding CPC class/subclass from DAV and/or CPC Tools (i.e., CAT, CPC Scheme Navigator, etc.,)

- H04L 63/08
- H04L 63/0853
- H04L 9/0863
- H04L 9/3228
- H04L 63/18

- G06F 21/34

- H04L 9/3234

- involving the use of external additional devices
- involving passwords or one-time passwords
- One-time or temporary data, i.e. information which is sent for every authentication or authorization, e.g. one-time-password, one-time-token or one-time-key
- using different networks or paths for security, e.g. using out of band channels (cryptographic
Plan and Execute Your Search

Understand invention
Plan and execute your search
Develop collection of terms
Perform preliminary search activities
Plan the Search

Inventive concept – Spec. vs. Claims – BRI of the Claims

**Inventive concept**

- Authenticate user using multi-channel Auth.
- Generate an OTP; Send the OTP to a registered device via out-of-band channel
- Receive a code/OTP from the 1st device; Authenticate user if the code matches with the OTP

**Limitations recited in the claims**

- Receive a login request from a first device
- Send auth. token to a registered mobile device
- Authenticate user based on response
- Multi-channel Auth. is recited in the preamble
- Generate an authentication token;
  - Send auth. token to a registered mobile device
- OTP and ‘out-of-band’ are not recited in the claim
  - Auth. token could be anything; It’s broader than OTP
- Receive a response;
  - Authenticate user based on the response
  - Token/OTP is sent from the 1st device is not recited;
  - Matching OTP is not recited in the claim;
  - A response in general - It’s not necessary the OTP
The Search Tree

Ways to narrow

- Add concepts
- Narrow concepts
- Change operators
  - \( \text{AND} \rightarrow \text{SAME/WITH} \)
- Limit by CPC
  - Groups/Subgroups
- Exclude concepts
  - Use NOT
- Reorganize concepts
- Limit by Date
- Many other options possible

References

Prior Art

Narrow Concepts

Refine Synonyms

Change Operators

Add Concepts

Searchable Indices

Limit by CPC

Inventive Concepts
A method for **authenticating a user using multi-channel authentication**, the method comprising:

1. receiving a **login request from a first device**, the login request includes user’s **credential**;
2. **in response to a verification that user's credential is valid**, generating an **authentication token**; and
3. **sending the authentication token to a registered mobile device**;
4. **receiving a response from the user**; and
5. **authenticating the user based on the received response**.
Plan the Search

Analyze claimed limitation for building Block Search

- Limitation 1: Multi-channel authentication
- Limitation 2: Login
- Limitation 3: create/send OTP to a registered device
- Limitation 4: receive OTP, Verify OTP for authentication

Search on Limitations 1, 3 and 4 would cover the claimed invention
Plan the Search

Building Block for Inventive Concept – Searchable Indices

Inventive Concept

Limitation 1

Multiple Channel Authentication

- Multiple channel
- Two/second channel
- Out-of-band, OOBA
- Multiple Factor, Different channel
- In-band

NEAR6

Authentication Authorization - Login

- Verify, Validate, Access Control

((multi$4 ADJ channel) (two ADJ channel) (second ADJ channel) (out$1of$1band) (out$ ADJ4 band)(OOB$1)) NEAR6 (authenticat$3 authoriz$5 log$3in$1) .ab,ti,bsum.
Plan the Search

Building Block for claimed limitations

**Limitation 3**

*in response to a verification that user’s credential is valid, generating an authentication token; and sending the authentication token to a registered mobile device;*

- **Sending**
  - Transmitting, Submitting, receiving
  - Communicating, Forwarding

- **NEAR6**
  - Token
    - PIN, OTP, code, One time password/code
    - Cookies, secret, key, nonce, ticket, pass-code, certificate, random, badge

- **WITH**
  - Device
    - Mobile, phone
    - PDA, laptop, handheld
    - PC, computer, wearable, tablet,

((validat$3 verify$3 authenticat$3 log$4in$1) NEAR6 (pass$1word$1 (pass ADJ word) credential user biometric)) WITH/SAME/AND

((send$3 transmit$4 submit$4 receiv$4) NEAR6 (token code PIN OTP (one ADJ time ADJ pass$6)) WITH (device mobile phone PDA laptop))
Plan the Search

Building Block for claimed limitations

Limitation 4: authenticating the user based on the received response;

NEAR6 MATCH
 Verify, Validate
 Compare, Valid

NEAR6 TOKEN
 PIN, OTP, code, One time password/code
 Cookies, secret, key, nonce, ticket, pass-code, certificate, random, badge

WITH authenticate
 Authorize, Login, Grant
 Validate, Verify, Access Control

((match$3 verify$3 validate$3) NEAR6 (token code PIN OTP (one ADJ time ADJ pass$6)) WITH (authenticate$3 authorize$5 grant$3))
Conduct Search
The Search Tree

Limit by Searchable Indices

S1 AND (H04L9/32$ H04L63/08$ G06F21/30-40 H04W12/06).CPC.

Limit by CPC

Multi channel authentication

Inventive Concepts

References

Prior Art

Multi Ch. Auth. CPC

Indices
The Search Tree

(S1 AND S2) AND (((multi$4 ADJ channel)(two ADJ channel)(second ADJ channel) (out$1of$1band)(out ADJ4 band)(OOB$1)) NEAR6 (authenticat$4 authoriz$5 log$4in$1)).ab,ti,bsum.

S1 AND (H04L9/32$ H04L63/08$ G06F21/30-40 H04W12/06).CPC

S1 (((multi$4 ADJ channel)(two ADJ channel)(second ADJ channel)(out$1of$1band) (out ADJ4 band)(OOB$1)) NEAR6 (authenticat$4 authoriz$5 log$4in$1))

Limit by CPC

Limit by Searchable Indices

Hits: 692 Relevant: At least 21

Hits: 1866 Relevant: at least 29

Hits: 3934 Relevant: at least 34
This reference fails disclose claimed limitations.

Although there are two authentication channels, the out of band authentication is entirely outside the user device and there is no discussion of Token/OTP!
This reference fails to disclose claimed limitations. Although there are two authentication channels, the out-of-band authentication is entirely outside the user device and there is no discussion of Token/OTP!

**Assessment:** - No discussion of Token/OTP

**Plan:** - Add limitation L3 to include Token/OTP
in response to a verification that user's credential is valid, generating an authentication token; and sending the authentication token to a registered mobile device;
The Search Tree

S3 AND ((validate$3 verify$3 authenticate$3 log$4in$1) NEAR6 (pass$1 word$1 (pass ADJ word) credential user biometric)) AND ((send$3 transmit$4 submit$4 receive$4) NEAR6 (token code PIN OTP (one ADJ time ADJ pass$6)) WITH (device mobile phone PDA laptop))
Beginning at block 356, a registration screen is displayed to a user at login. In some embodiments, the following logic may be invoked only upon receipt of proper login name and password and verification that the previously deposited cookie is present on the user’s machine in accordance with above principles.

FIG. 13 shows how a one-time pass code can be delivered to a user by means of IVR. In summary, the IVR feature may place an outbound call and transmit a spoken one-time pass code to a wireless or land line phone that has been pre-registered by the end user. The phone will take the following actions upon:

[0066]

[0074]
Beginning at block 356, a registration screen is displayed following login name and password previously entered into the machine input screen.

**Assessment:** - Two steps “verifying login name-password” and “transmitting one-time pass code” are not in context.

**Plan:** - Replace operator “AND” by “SAME”
The Search Tree

**S5 AND**

\[(\text{match}\,3\,\text{verify}\,3\,\text{validat}\,3)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{authenticat}\,3\,\text{authorize}\,5\,\text{grant}\,3)\]

**S6**

Add Concepts

**S3 AND**

\[(\text{validat}\,3\,\text{verify}\,3\,\text{authenticat}\,3\,\text{log}\,4\,\text{in}\,1)\,\text{NEAR}\,6\,(\text{pass}\,1\,\text{word}\,1\,\text{pass ADJ word) credential user biometric})\,\text{SAME}\]

\[(\text{send}\,3\,\text{transmit}\,4\,\text{submit}\,4\,\text{receive}\,4)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{device mobile phone PDA laptop})\]

**S5**

**S5 AND**

\[(\text{match}\,3\,\text{verify}\,3\,\text{validat}\,3)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{authenticat}\,3\,\text{authorize}\,5\,\text{grant}\,3)\]

**S6**

Add Concepts

**S3 AND**

\[(\text{validat}\,3\,\text{verify}\,3\,\text{authenticat}\,3\,\text{log}\,4\,\text{in}\,1)\,\text{NEAR}\,6\,(\text{pass}\,1\,\text{word}\,1\,\text{pass ADJ word) credential user biometric})\,\text{SAME}\]

\[(\text{send}\,3\,\text{transmit}\,4\,\text{submit}\,4\,\text{receive}\,4)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{device mobile phone PDA laptop})\]

**S5**

\[S5\,\text{AND}\,(\text{match}\,3\,\text{verify}\,3\,\text{validat}\,3)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{authenticat}\,3\,\text{authorize}\,5\,\text{grant}\,3)\]

\[S6\]

Add Concepts

**S3 AND**

\[(\text{validat}\,3\,\text{verify}\,3\,\text{authenticat}\,3\,\text{log}\,4\,\text{in}\,1)\,\text{NEAR}\,6\,(\text{pass}\,1\,\text{word}\,1\,\text{pass ADJ word) credential user biometric})\,\text{SAME}\]

\[(\text{send}\,3\,\text{transmit}\,4\,\text{submit}\,4\,\text{receive}\,4)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{device mobile phone PDA laptop})\]

**S5**

**S5 AND**

\[(\text{match}\,3\,\text{verify}\,3\,\text{validat}\,3)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{authenticat}\,3\,\text{authorize}\,5\,\text{grant}\,3)\]

\[S6\]

Add Concepts

**S3 AND**

\[(\text{validat}\,3\,\text{verify}\,3\,\text{authenticat}\,3\,\text{log}\,4\,\text{in}\,1)\,\text{NEAR}\,6\,(\text{pass}\,1\,\text{word}\,1\,\text{pass ADJ word) credential user biometric})\,\text{SAME}\]

\[(\text{send}\,3\,\text{transmit}\,4\,\text{submit}\,4\,\text{receive}\,4)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{device mobile phone PDA laptop})\]

**S5**

**S5 AND**

\[(\text{match}\,3\,\text{verify}\,3\,\text{validat}\,3)\,\text{NEAR}\,6\,(\text{token code PIN OTP (one ADJ time ADJ pass}\,6))\,\text{WITH}\,(\text{authenticat}\,3\,\text{authorize}\,5\,\text{grant}\,3)\]
Assessment:

This reference fails disclose claimed limitations as user’s credential and OTP are submitted at the same time.
The reference reads on the current claim:

However, it does not encompass inventive concept as the OTP is received at and sent from the OOB device (i.e., registered device).

[0056] This process begins at block 475, where a request is sent to a backend entity for an OOB authorization. In an embodiment, this request may be sent via the application. Next at block 480 the client system receives an OOB authentication code from the associated mobile device (referred to herein as an OOB device, as this device and communications between the client system and this device are separate from and thus out-of-band to communications between the client system and the backend entity).
This appears to be an anticipatory reference!
This appears to be another anticipatory reference!

**SHOULD WE STOP SEARCHING?**

**SHOULD CONDUCT A COMPLETE AND THOROUGH SEARCH**
The Search Tree

Prior Art
- Add Concepts
- Narrow Concepts
- Refine Synonyms
- Change Operators
- Add Concepts
- Searchable Indices

Inventive Concepts

References

S6: Inv+CPC+Indices
Send OTP
Ver. OTP

S6: Hits: 101 Relevant: 16

TC 2400 - Prior Art Search 2.0
Multi channel authentication

in response to a verification that user’s credential is valid,
generating an authentication token; and
sending the authentication token to a registered mobile device;

authenticating the user based on the received response;
The Search Tree

**S8**

**AND**

**((match$3 verify$3 validat$3) NEAR6 (token code PIN OTP (one time ADJ pass$6)) WITH (authenticat$3 authoriz$5 grant$3))**

**S7**

**AND**

**((validat$3 verify$3 authenticat$3 log$4in$1) NEAR6 (pass$1word$1 (pass ADJ word) credential user biometric)) SAME**

**((send$3 transmit$4 submit$4 receiv$4) NEAR6 (token code PIN OTP (ADJ time ADJ pass$6)) WITH (device mobile phone PDA laptop))**

**S1**

**AND**

**(((multi$4 ADJ channel)(two ADJ channel)(second ADJ channel)(out$1of$1 (out ADJ4 band)(OOB$1)) NEAR6 (authenticat$4 authoriz$5 log$4in$1))**

References
Conduct Search – Text Search

Review and Tag References

Pub. No.: US 2011/0302641 A1
Pub. Date: Dec. 8, 2011

Fig. 1

TC 2400 - Prior Art Search 2.0
[0023] The first embodiment contemplates a Server-possession process, as is further shown in FIG. 2. According to the method, the Authentication Server 131 sends an out-of-band Authentication notice (ANM) 140 via short message service (SMS) or other suitable technology to an SMS capable device 150 (such as a cell phone, pager, PDA, radio) or interactive voice response (IVR) call to a pre-registered device (such as a cell phone, home phone, or office phone). This ANM token 170 transaction is being conducted and prompts him to enter an Authentication & Key Server 131, if properly validated, a one-time-passcode (OTP) 180 is distributed by the Authentication and Key Server 131 to the user via the pre-registered device (150 or 160) that was just previously validated in their possession. This OTP is then entered by the User to complete the transaction.
Conduct Search
Monitor and Adjust Search

Identify Other Terminologies from Relevant References

Modify Search using the Identified Terminologies

Continue monitoring and adjusting search
Conduct Search – Monitor and Adjust Search
Identify Other Synonyms/Terminologies recited in Relevant Art

Pub. No.: US 2013/0225128 A1
Pub. Date: Aug. 29, 2013

[0008] FIG. 6 illustrates a somewhat improved authentication approach that uses out-of-band communication, known as server-generated one-time password (OTP) authentication. Again, user 520 requests some action to be taken using interface 611 on

[0125] One way to reduce the problems inherent in performing voice biometrics on mobile devices (or in conjunction with the use of mobile devices) is to eliminate the inaccuracy that may occur during attempts (because of the problem cited above wherein the channel acoustic characteristics from the channel that allows mobile device-based voice rec

Another synonym for Multi-Channel Authentication
Conduct Search – Monitor and Adjust Search

Identify Other Synonyms/Terminologies recited in Relevant Art

Assessment: - Found another synonym for ‘multi-channel authentication’

Plan: - Update search using newly found synonym
Conduct Search – Monitor and Adjust Search

Update Search On New Synonyms/Terminologies

Conduct search on newly found synonyms

Review and Tag References!
Conduct Search – Monitor and Adjust Search

Conduct Search On Newly Found Synonyms

(19) United States
(12) Patent Application Publication
Gill et al.

(10) Pub. No.: US 2015/0215310 A1
(43) Pub. Date: Jul. 30, 2015

SYSTEM AND METHOD FOR CROSS-CHANNEL AUTHENTICATION

Another good art for a rejection!

TC 2400 - Prior Art Search 2.0
Monitor/Adjust Search – Tips and Hints

Reduce # of Hits (Narrow Search)

Narrow concepts/queries by:

- Adding more terms into a phrase/sentence using “NEAR” and/or “WITH”
- Using less synonyms
- Adjusting proximity of the operator and/or wildcards
  
  Ex. “AND” → “SAME”/“WITH”; “WITH” → “NEAR”; “NEAR6” → “NEAR3”

Combining more concepts/limitations/phrases/sentences by:

- Concatenating more limitations/phrases/sentences using “AND”

Increase # of Hits (Broad Search)

Broaden concepts/queries by:

- Removing search terms from search strings (i.e., phrases/sentences)
- Using more synonyms
- Increasing proximity of the operators and/or wildcards
  
  Ex. “WITH” → “SAME”; “NEAR” → “WITH”; “NEAR3” → “NEAR7”

Combining less concepts/limitations/phrases/sentences
Conduct Search – Monitor/Adjust Search

Check if any terminologies are not included in search terms

During reviewing relevant references, verify if any terminologies are NOT included in current search strings
Adjust search strings accordingly

Forward/Backward Recitation Search

Perform “Forward/Backward Recitation Search” on relevant references using .URPN. search

Exhausting Search

Think how to properly split limitations and combine references (i.e., do 103 rejection instead of 102)