Inventions on LDAP security- A TRIZ based analysis

Umakant Mishra
Inventions on LDAP security

-A TRIZ based Analysis

By- Umakant Mishra, Bangalore, India

http://umakantm.blogspot.in

Contents

Contents ........................................................................................................................................... 1
1. Introduction ................................................................................................................................... 2
2. Study on Inventions on LDAP Security ............................................................................................... 2
  2.1 Objectives of the study ................................................................................................................. 2
  2.2 Major areas of Invention ............................................................................................................... 3
  2.3 Patents analyzed for the study ..................................................................................................... 3
3. LDAP security and authentication mechanism ...................................................................................... 4
4. Major Concerns in LDAP security ....................................................................................................... 5
5. IFR for LDAP data security ............................................................................................................... 6
6. Inventions LDAP data Security ........................................................................................................... 7
  6.1 Method of securing sensitive data in LDAP directory ................................................................. 7
  6.2 Using non-local data within a LDAP environment for security and authentication ......................... 7
  6.3 Policy validation in a LDAP directory ............................................................................................ 9
  6.4 Trusted processing of Unique Identifiers in LDAP ....................................................................... 11
7. Other related inventions .................................................................................................................... 11
  7.1 Open architecture global sign-on method ....................................................................................... 11
  7.2 Storing sparse hierarchical ACL data in RDBMS for LDAP .................................................... 12
  7.3 Processing sparse hierarchical ACL data in RDBMS ................................................................. 12
  7.4 Providing extendible Access Control for LDAP Protocol ......................................................... 12
  7.5 Storing Policies in LDAP for policy-based management .............................................................. 13
  7.6 Simplified LDAP access control language system ....................................................................... 13
  7.7 Incorporating filtered Roles in LDAP ......................................................................................... 13
8. Summary and Findings of the study .................................................................................................... 14
  8.1 Distribution of patents ................................................................................................................ 14
  8.2 Hot areas in LDAP security ...................................................................................................... 14
  8.3 Trends of evolution in LDAP security ........................................................................................ 14
  8.4 Predicting future inventions on LDAP security ........................................................................ 15
Reference to patents: ............................................................................................................................ 15
Other references: ............................................................................................................................... 16
1. Introduction

Lightweight Directory Access Protocol (LDAP) is an IETF open standard to provide directory services in the network. LDAP was initially developed at the University of Michigan with an objective to include most of the features of X.500 directory system, while eliminating the burdens and limitations of the same.

The current Version of LDAP is LDAP V.3 released in December 1997 (RFC 2251). Other specifications of LDAP can be found in different RFCs on the IETF (Internet Engineering Task Force) website.

With the growing use of Internet, LDAP is becoming more and more popular to provide directory services to a wide range of applications. This led to patenting several inventions relating to LDAP operation and application. This article on LDAP data security is a part of the main study on “Inventions on LDAP” based on 60 selected patents from US Patent database.

2. Study on Inventions on LDAP Security

This study on LDAP security is a part of the above-mentioned study on “Inventions on LDAP”. The study is mainly based on the analysis of US patents. The objectives and the methodology of the main study is presented in the article mentioned above. The details on this part of the study relating to LDAP security are as below.

2.1 Objectives of the study

- The objective of the study is to know- what are the inventions made on LDAP security and on which aspects of security?

- What is the Ideal Final Result (IFR) in the issues relating to security in LDAP directory? Is there any trend in the inventions on implementing security in LDAP?

- Which problems on LDAP security are not solved yet? In other words which problems need to be addressed in future?

- Which aspects of LDAP security are yet unexplored? What are the possible areas of improvements in future inventions?
2.2 Major areas of Invention

- One major area that attracts the inventors is to implement security for LDAP data. In a distributed environment the data may be fragmented across multiple machines where the security becomes a big concern.

- Another area of invention is related to the client authentication at LDAP server. The server should allow only authorized clients to access the data and protect it from the intruders. Besides, authentication becomes critical especially when an LDAP server searches a referral query on multiple directories.

- The other important area is implementing security at the client. The client may have some sensitive data, which he may not like to share with public.

- Yet another area that attracts inventors is to store the Access Control List (ACL) data in the RDBMS used for storing LDAP data.

- Another area that attracts inventors is to implement user groups and policies. The user groups and policies restrict the access of the users to the LDAP directory.

2.3 Patents analyzed for the study

The study analyzes the following four patents, which deal with the issues on LDAP security.

- US Patent 6339827, “Method for securing sensitive data in a LDAP directory service utilizing a client and/or server control”

- US Patent 6581093, “Policy validation in a LDAP directory”,

- US Patent 6708170, “Method and system for usage of non-local data within a lightweight directory access protocol directory environment”,


Besides the following patents are also found to be relevant to this topic of maintaining security in LDAP and analyzed in brief.

- US Patent 6801946, “Open architecture global sign-on apparatus and method therefore”.

- US Patent 6708170, “Method and system for usage of non-local data within a lightweight directory access protocol directory environment”,

Inventions on LDAP security- A TRIZ based analysis, by Umakant Mishra
3. LDAP security and authentication mechanism

The LDAP server stores directory information in a backend database. The client makes a TCP/IP connection and sends requests to an LDAP server. The LDAP server authenticates the client and does the necessary operation based on client’s requests. Finally the LDAP server returns a response containing any results or errors to the requesting client. LDAP servers provide their service using a default port 389.

The specifications of LDAP v.3 provide facilities for simple authentication using a cleartext password as well as any SASL mechanism. SASL allows for integrity and privacy services to be negotiated (RFC 2251, www.ietf.org/rfc/rfc2251.txt).

Use of cleartext password is strongly discouraged where the underlying transport service cannot guarantee confidentiality and may result in disclosure of the password to unauthorized parties.

The protocol allows other security mechanisms like SASL to be implemented in LDAP. The protocol also permits that the server can return its credentials to the client, if it chooses to do so.

Inventions on LDAP security- A TRIZ based analysis, by Umakant Mishra
One method of controlling user access to the directory services is through Access Control Lists (ACL) for Distinguished Names (DN). Such implementations typically link a DN (or user) to a particular access group, where the group is granted a particular set of permissions for accessing the directory services.

Another method of restricting the sensitive data is to assign security classifications based on the attribute rather than the Distinguished Name (DN). For example, attributes (like telephone number or bank a/c number) may be classified as sensitive, so that the they are not available to public but restricted to specific groups of users only.

4. Major Concerns in LDAP security

- There is no standard method of controlling user access to LDAP directories. Although Access Control Lists (ACL) have been used in conjunction with LDAP, they have very limited scope.

- Although LDAP protocol specifications allow other security mechanisms to be implemented with it, most of them do not match so well to go with LDAP.

- Data in LDAP is stored in clear-text format, which is not suitable to store confidential data such as passwords.

- It is difficult to store Access Control List (ACL) data in RDBMS which is often preferred as LDAP backing store for its proven advantages.

- Authenticating users in a distributed environment remains a concern. It is always a debate whether to authenticate the user by one master server (where authentication will be slow), or to store user information in every participating server (redundant storage with data replication) or to follow any other authentication strategy.

- The referral mechanism of LDAP sends queries to other LDAP servers where authentication becomes an issue.

- Each data in LDAP cannot be made available to public. It is necessary to implement user groups and user policies to restrict access to LDAP database.
5. IFR for LDAP data security

According to TRIZ, ideality is a function of its benefits and costs. **Ideality = \( \frac{\Sigma Benefits}{\Sigma Costs + \Sigma Harm} \).** So the Ideal Final Result in LDAP security can be achieved by increasing all useful functions of the data security and decreasing all harmful functions of the same. An analysis of the LDAP system may find the following as IFR for LDAP security.

<table>
<thead>
<tr>
<th>Should have (Positive features)</th>
<th>Should not have (Negative features)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The LDAP server should authenticate the user and restrict its data only to the authorized users.</td>
<td>LDAP should not allow unauthorized users to access data from the directory.</td>
</tr>
<tr>
<td>The LDAP user should be able to define the confidentiality of specific data items and should be able to restrict his data to specific user groups.</td>
<td></td>
</tr>
<tr>
<td>The user authorization should take minimum time. There should be a mechanism to authenticate user even in distributed environment.</td>
<td></td>
</tr>
<tr>
<td>The LDAP may store its data in encrypted format to maintain confidentiality.</td>
<td>The security mechanism should not increase complicacy of the system.</td>
</tr>
<tr>
<td>LDAP should be able to store Account Control Lists (ACL) to protect enable access rights to the users. It should preferably store ACL with the data it protects.</td>
<td>The language to define Access Controls should not be difficult for users.</td>
</tr>
<tr>
<td>There should be user policies and groups to exactly define the scope of accessibility to specific data items.</td>
<td></td>
</tr>
<tr>
<td>LDAP should support the existing methods of data security.</td>
<td></td>
</tr>
</tbody>
</table>
6. Inventions LDAP data Security

As we discussed above the LDAP specification allows other security mechanisms to be implemented along with. But in many cases the existing security and authentication mechanisms may not be suitable for an LDAP environment. That is where a number of inventors have put their efforts.

6.1 Method of securing sensitive data in LDAP directory

Background Problem:
The LDAP directory stores various data on users, computers and various other objects in the network. It also stores confidential data as well. Unfortunately, the present implementation of LDAP does not have a security mechanism. The data is stored in clear-text form or in “as is” format. This is not suitable to store confidential data such as passwords. There is a need to provide security to store and retrieve sensitive data in LDAP.

Solution by US Patent 6339827

US Patent 6339827 discloses a method of maintaining security in a directory service. As per the invention the lightweight directory access protocol (LDAP) is extended to include two controls, one client-control and one server-based control for securing sensitive data in the directory service.

According to the invention, the client control is to be implemented on a client machine, and/or the server control is to be implemented on the server machine. The client control will comprise a control block including identification information, a signature control block and a digital signature. This provides security to the sensitive data provided from a client application to the directory service. The server side control similarly includes necessary controls to provide security for the data within the directory service.

The invention is flexible to activate either client-control or server-control or both. In other words, it is not required to have both client and server controls to be implemented together. A client machine may implement the client control irrespective of whether a server involved in the directory operation is running the server control.
TRIZ based analysis

The invention proposes two controls, viz., a client-control to be implemented on the client machine and a server-control to be implemented on a server machine (Principle-1: Segmentation).

According to the invention, the client control will include necessary mechanism to provide security to the sensitive data at the client side, and the server side control will include necessary mechanism for the security of data within the directory service (Principle-3: Local Quality).

Both controls can be independently activated. A client machine may implement the client control irrespective of whether a server involved in the directory operation is running the server control (Principle-15: Dynamize).

6.2 Using non-local data within a LDAP environment for security and authentication

Background problem:

LDAP provides a mechanism for searching other directories through a referral. When LDAP does not find the result of the query in its directory, it may return a reference to another server (or set of servers), which may be accessed via LDAP or other protocols. The client may use that referral to contact other servers. But the problem is, the LDAP servers contacted through referral may not recognize the client’s registry information as the client belongs to a different LDAP server. It is necessary to have authentication mechanism for clients accessing multiple referral servers.

Alternative solutions:

One approach to solve authentication problem is to use a client push model as found in the Distributed Computing Environment (DCE) developed by the Open Group. In this approach, the user registers with a first server and receives credentials (Principle-10: Prior Action). These credentials are presented for accessing the second server. The second server either accepts or denies the credentials after verification. Windows NT also uses a similar client push model.

Another approach is to define all user and group information on each machine as done in a LAN. Each server in the domain maintains a copy of authentication information (Principle-26: Copying). But this method uses excess space and administrative problems when the directory is distributed over multiple servers.

Let LDAP server search the query in other servers (Principle-25: Self Service). But that will put excessive load on the LDAP server.
All these solutions have drawbacks to be implemented on an LDAP server. It is necessary to find an improved method that allows an LDAP server to use the resources on another LDAP server.

**Solution provided by US Patent 6708170:**

US Patent 6708170 finds a method of maintaining authentication information in a distributed network of servers using LDAP directories. According to the invention the local LDAP server generates and maintains a non-local access server list. It also queries the non-local servers and caches the responses from each queried server.

When a request to authenticate a user with a distinguished name is received, the local access control data and the cached directory are searched for the distinguished name. If the distinguished name is located, the user is authenticated with each server in the non-local access server list.

**TRIZ based analysis**

According to the invention the local server queries the non-local servers and caches the responses (Principle-10: Prior Action, Principle-26: Copying).

When a request for authentication is received, the server also searches the cached directory (Principle-27: Cheap and short-living objects) as against searching the non-local servers.

Once the distinguished name is located, the user is authenticated with each server in the non-local access server list (Principle-6: Universality).

**6.3 Policy validation in a LDAP directory**

**Background problem:**

It is necessary to validate the network resources to ensure security. But it is not possible to implement full validation policies for many network devices due to serious memory and computation power limitations. In those cases, a partial validation is advisable to be implemented. There is a need for a flexible validation
method that should enable efficient validation schemes in a secure environment and secure validation schemes in an insecure environment.

**Solution provided by US patent 6581093:**

US Patent 6581093 proposes a method of policy validation in a LDAP directory. According to the invention, the policies are stored in a directory as entries. Each entry has multiple attributes, which are used for validation of the resource.

A record validator creates and stores a set of record validation information in the LDAP server. The validation information records may include the modification or creation time of the validated records. The network elements in a resource-constrained network verify the validation information records instead of going through validation process. The network elements compare the time stored in the validation information records to the actual modification or creation time of records to verify validity information. This method of verifying the validation information is much simpler than the validation method.

**TRIZ based analysis**

It is necessary to validate the network resources to ensure security. But resource-constraint networks do not afford full validation policies for many network devices due to memory and bandwidth limitations (Contradiction).

According to the invention, a record validator creates and stores a set of record validation information in the LDAP server (Principle-10: Prior Action).

In a resource-constraint network, the network elements verify the validation information records instead of going through the full validation process (Principle-26: Copying).
6.4 Trusted processing of Unique Identifiers in LDAP

**Background problem:**
Many security systems are moving their databases to LDAP. But each of those security systems must store and protect its own set of unique identifiers on LDAP. A unique identifier is unique within the database of a security system, usually created by the security system while adding a user or group. When the security systems move to LDAP they create, store and take precautions to protect their unique identifiers, as LDAP does not provide any mechanism to generate, verify or protect a unique identifier. It would be nice to have a common set of unique identifiers, which could be shared by different security systems using the LDAP directory.

**Solution provided by Patent 6714930**
US Patent 6714930 presents a method, which allows different security systems to store and retrieve unique identifiers that are shared or common to the entire directory. According to the invention, there will be a trusted process, which will allow LDAP users to store and retrieve unique identifiers using standard LDAP interfaces. The trusted process generates or verifies a unique identifier, guarantees the uniqueness of a unique identifier within the entire directory (rather than just within a single security system), and guarantees that any unique identifier returned to an LDAP user is a trusted unique identifier.

**TRIZ based analysis**
The invention generates unique identifiers and guarantees the uniqueness of the unique identifier within the entire directory and allows all the security systems to share the unique identifier information (Principle-6: Universality).

7. Other related inventions

7.1 Open architecture global sign-on method
A global sign-on technology allows all of the user Identifiers (UID) and passwords to be maintained automatically by the global sign-on system (GSO). There is a need for a GSO in an open architecture environment such as Internet while ensuring the security afforded by a distributed computing environment.

US Patent 6801946 discloses a method of implementing a global sign-on using LDAP. Users in an enterprise-computing environment typically access several different systems each having unique user-id and password. The invention maintains a GSO database in an LDAP server. The user login once into the GSO and automatically authenticated in all other systems (Principle-6: Universality).
7.2 Storing sparse hierarchical ACL data in RDBMS for LDAP

Security for LDAP is provided through ACLs (Access Control Lists). These ACLs need to be stored in the RDBMS along with the data it protects. US Patent 6438549 discloses a method of securing sparse Access Control List (ACL) data in a relational database used as a backing store for LDAP. According to the invention the ACL data is stored in multiple tables, such as an owner table, a propagation table, a permissions table and a source table (Principle-24: Intermediary, Principle-1: Segmentation). The owner table stores data objects with explicitly set ACLs. The propagation table stores data on whether individual ACLs are inherited by descendant objects. The permissions table store data regarding permissions and the source table stores data for a set of ancestor objects having respective ACLs for each of a set of descendant objects. This method reduces the activities involved in searching and updating ACL.

7.3 Processing sparse hierarchical ACL data in RDBMS

US Patent 6823338 discloses a method for processing Access Control List (ACL) for LDAP in a relational database. This method is similar to the above invention (patent 6438549, by the same inventors), which stores ACL data in multiple tables, such as an owner table, a propagation table, a permissions table and a source table (Principle-1: Segmentation). According to the invention, the first three tables are used to determine the entry owner and ACL for a given object. Whereas the fourth table (the source table) significantly increases the search speed.

When a SELECT operation is performed based on an identifier of the object, if an ACL or owner is found, that value is kept. If, however, either the ACL or owner is not determined, the parent is checked. If the needed value is then found, a propagation flag is checked. If the propagation flag is TRUE, that value is kept. If the propagation flag is FALSE, then processing continues recursively until both an owner and an ACL value have been found (Principle-20: Continuity of useful action). If the top of the tree (the suffix) has been reached without locating a propagating value, then system defaults are returned (Principle-11: Cushioning).

7.4 Providing extendible Access Control for LDAP Protocol

US Patent 6633872 provides a method of providing extendible access control to LDAP protocol. According to the method, after the LDAP server authenticates the user, the user is associated to a particular access control group (Principle-35: Parameter change). The access control group may include several application specific parameters, which may include security levels, permissions or access rights.

After the user is associated with an access control group, the LDAP operation is reformatted (Principle-28: Mechanics Substitution) based on the parameters in the access control group and provided to the search engine. The extendible ACL can be implemented as a plug-in within the scope of LDAP server.
7.5 Storing Policies in LDAP for policy-based management

Every network follows certain protocols, which consists of a set of rules defining how entities interact with each other. Every hardware and software (and even others) has to follow the policies and protocols for effective interaction in the network. Currently the application programs that execute in network devices rarely invoke QoS functions, and therefore they do not take full advantage of QoS features that are available in the network devices. There is a need to integrate applications into a policy-based networking system.

Patent 6463470 discloses a method of storing policies in LDAP in the form of policy statements. An application program and the policy server network device can retrieve the policy information from the Repository using LDAP protocol. Thus the Policies are in easily accessible format (Principle-33: Homogeneity) and available in a commonly accessible place (Principle-6: Universal).

7.6 Simplified LDAP access control language system

US Patent 6950819 provides a simplified LDAP access control system. The system provides a simplified language (Principle-28: Mechanics substitution), using which the system administrator can give a user the flexibility to specify a list of people whom he allows to read or write his information. Thus the system administrator need not write ACL for all the users. This makes the system administrator write the general rules of ACL and the users write the user level rules (Principle-1: Segmentation). The ACLs are stored in the directory along with the entries. The server allows access to that entry based on the attributes specified in the ACL.

7.7 Incorporating filtered Roles in LDAP

Roles are often useful to filter specific entries. But a typical directory tree organizes entries only hierarchically, which is not suitable to implement groupings based on roles. US Patent 6768988 discloses a method of implementing Roles in LDAP. According to the invention, the roles are defined by role definition entry. The roles use an LDAP filter in order to search a designated portion of the directory system and to identify those entries that possess the characteristics described in the filter (Principle-1: Segmentation). Once the roles are defined the client application can perform various operations on the roles, such as, enumerating members of the role, obtaining a list of role members, assigning a particular role to a given entry, removing a particular role from a given entry and so on. The invention allows creating nested roles by creating roles that contain other roles.
8. Summary and Findings of the study

8.1 Distribution of patents

- A total of eleven patents are illustrated in the study, out of which four patents are found to be more relevant to LDAP security compared to others. The four patents, which are found to be more relevant for LDAP security, are analyzed in detail. The rest seven patents are presented in brief.

- All of the four illustrated patents are assigned by IBM (International Business Machines). IBM is found to be the major assignee in this field.

- There are a large number of patents on data security in general. Although, those inventions in data security are also applicable for LDAP data security, those patents are considered out of the scope of this study.

8.2 Hot areas in LDAP security

The analysis finds that the inventions try to improve the following aspects of LDAP system.

- Improving user authentication in heterogeneous environment.

- Faster authentication in distributed LDAP environment.

- Storing and managing ACLs in RDBMS.

- Separating and integrating security at the client and the server end.

- Authentication mechanism in referral services.

- Generating single login and/or unique identification for different security systems using LDAP.

8.3 Trends of evolution in LDAP security

The following trends are prominent in the inventions on LDAP security.

- Increasing speed in LDAP authentication - Inventions want to increase speed of authentication in large distributed environment.

- Increasing controllability- Inventions want to integrate user authentication with policies and groups so that the sensitive data is restricted to specific users and not available to the public.
- Increasing easiness to “configure and implement” and increasing easiness to “maintain and administer” are two obvious trends.

- Increasing standardization- Inventions are looking for Increasing interoperability to facilitate integration with other systems, databases or services, supporting conversion and migration.

8.4 Predicting future inventions on LDAP security

Based on the analysis we can predict more inventions on the following aspects of LDAP security in future.


- Single login and authentication for multiple LDAP servers (Principle-6: Universality).

- Optimizing client security system (Principle-3: Local Quality).


- Allowing users to configure access rights to their own data (Principle-3: Local Quality, Principle-15: Dynamization).


There are many more possible areas of development in the field of LDAP security. The future days will show many more inventions in this field.

Reference to patents:


Other references:

12. Umakant Mishra, Inventions on LDAP- a Study Based on US Patents  
   http://works.bepress.com/umakant_mishra/52

13. Umakant Mishra, Inventions on LDAP data storage- A study based on US patents, (Sept 20, 2006),  
   http://papers.ssrn.com/abstract=931224

14. Umakant Mishra, “Inventions on LDAP data storage- a TRIZ based Analysis”,  
   http://papers.ssrn.com/abstract=925921

15. Umakant Mishra, Inventions on LDAP Data Management - A TRIZ Based Analysis (August 2006). Available at SSRN:  
   http://ssrn.com/abstract=925931

16. Umakant Mishra, Inventions on LDAP Administration- A TRIZ Based Analysis (August 2006). Available at SSRN:  
   http://ssrn.com/abstract=925932

17. Umakant Mishra, Inventions on Data Searching in LDAP - A TRIZ Based Analysis (August 2006). Available at SSRN:  
   http://ssrn.com/abstract=925935

18. Umakant Mishra, Inventions on Extending LDAP Functionality - A TRIZ Based Analysis (August 2006). Available at SSRN:  
   http://ssrn.com/abstract=925941

19. Umakant Mishra, Inventions on Integrating LDAP with Other Directories - A TRIZ Based Analysis of US Patents (August 2006). Available at SSRN:  
   http://ssrn.com/abstract=925943

20. US Patent and Trademark Office (USPTO) site,  
   http://www.uspto.gov/  

   Wahl, Howes & Kille, Dec. 1997,  