Global Information Assurance Certification Paper

Securely Implementing LDAP
Ellen Smith
July 29, 2001

LDAP Directories are increasingly prevalent in corporate environments. They are used as public sources of information, much like telephone books, and as storage for authentication credentials. Some directories are also being used to manage network resources.

Risk is a product of threat, vulnerability, and cost. However, always keep in mind that anything times zero is zero. Even though the level of confidentiality of the data in a public directory may be very low, the integrity of that data always needs to be protected. Thus, we always need to factor in security considerations in our LDAP implementations. This paper will discuss the various security exposures and possible solutions when implementing LDAP directories. For a good overview of LDAP itself, please see the web articles, "LDAP: Use as Directed" by Tim Howes, and "Overview & Security Aspects of the Lightweight Directory Access Protocol (LDAP)" by Louis R. Brand.

The first consideration when implementing security should always be to ask, "What is being secured from what?" – Is the data sensitive? Is it vulnerable to unauthorized access or modification? Must the requester of the information be identified? The following chart, taken from a presentation by Jeff Hodges, shows some possible security considerations resulting from answers to those questions.

Another question to address is, "How available must this data or system be?" – Does it impact other systems? Would denial of service be a problem?

scenarios	Contains Sesitive Data?	Connection Hijacking or IP Spoofing Threats?	Anonymous Requesters?		Identified Requesters?		Required Directory-Specific Security Mechanisms or Functions
				Read/Write ?		Read/Write ?	
1	N	N	Y	RO	N		None
2	N	N	N	N/A	Y	RO	Secure Authentication
3	N	Y	N/A	N/A	N/A	N/A	Mutual authentication, Connection Integrity-Protection
4	N	N	Y	RO	Y	RW	Secure Authentication
5	Y	Y	N/A	N/A	N/A	N/A	Mutual authentication, Connection Integrity- and Confidentiality-Protection

Security Exposures with LDAP

Denial of Service (DoS) - Directories centralize information, making timely access to that information critical. Thus, Denial of Service (DoS) attacks become a real threat for the directories.

Confidentiality refers to preventing, detecting, or deterring the improper disclosure of or access to information. This is important when the data in a directory is sensitive and should not be disclosed in a general fashion. Encryption is used to supply confidentiality. LDAP supports SSL, which can be used for client-server encryption.

Integrity refers to preventing, detecting, or deterring the improper modification of information. Regardless of the level of confidentiality of data in a directory, the integrity of that data is always a concern. SSLv3.0 can again be used to meet this requirement. In addition, digital signatures

can protect against the Man-in-the-Middle attack. Certificates that expire after six months are also helpful in order to reduce the likelihood of the certificate being compromised. Finally, Access Control can be used to more granularly limit the modification of information. Although this is not yet standardized with LDAP, most directory products implement this feature in some way.

Authentication refers to confirming identity. There are three levels of authentication provided with LDAP:

> None – provides anonymous connections, thus no authentication. This is appropriate for general, read-only directories.
>
> Simple – provides connections based on a user name or ID and password. In LDAP the password can be stored in clear-text or hashed. This is appropriate when anonymous users are not allowed access to the directory, or when particular users have special privileges in the directory.
>
> Strong – Certificates or public keys are used for strong identification. LDAP can store public keys or certificates and use SSL for transport. In addition, LDAP supports SASL for mutual authentication. This is appropriate for securing communication between directories and applications.

Authorization refers to determining appropriate credentials or granting access rights to properly authenticated individuals. This is typically done via Access Control. Access Control is not defined in the LDAP standard, so its implementation is specific to each particular LDAP product.

Non-repudiation refers to being able to prove in a court of law that someone actually sent a piece of information (the sender, and no one but the sender, sent the message.) Digital signatures are usually used to meet this requirement. Although LDAP has no provision for this, the use of digital signatures with SSL or the use of XML can provide this need.

Currently, few implementations of LDAP require this. However, many sensitive applications require non-repudiation, and it is necessary to establish this at the beginning of a session when a user authenticates.

Backdoor Access refers to the ability of someone on the network or with physical access to the server to retrieve information directory from the disk. The confidentiality and integrity of stored data must also be protected from this type of access. LDAP, as a protocol, cannot protect against this risk, but other network and host security measures can.

Security Solutions with LDAP

LDAP has a few standards which help to secure directories. Access Control and Replication are not yet standardized, but many LDAP products implement these important features in some manner. Security in any system is never assured, but is usually increased by layers.

Gateway Layer

The first security layer to consider is the gateway. This answers the question, "Who is allowed on the system?" It is typically a network-level security that includes physical access, firewalls and VPNs. As this layer should be considered whether or not LDAP is being used, details will not be provided here. Intrusion Detection Systems, both network and host-based are helpful at this level to alert the administrator to a breach at the gateway. Here is a short list of items to consider that would affect a directory:

- Restrict physical access to servers.
- Disable all unused ports.
- Harden the OS on servers according to vendor specifications.
- Install the latest patches.
- Install network-based intrusion detection systems.

If there is no need to identify requesters of information in the directory, this may be adequate. Otherwise, you may also want to secure channels between the application host and LDAP. (See section below.)

This is also the layer that needs to protect against Denial of Service (DoS) attacks, so take care to configure the firewalls appropriately. If a DoS attack does get through the gateway layer, the resulting damage may be somewhat minimized at the control layer.

Control Layer

The second layer to consider is the control layer. This layer answers the question, "What may be accessed on the system?" Determine the necessary security functions based on the need for confidentiality and integrity of the data. Also consider the threat of someone hijacking or spoofing the IP address of your directory to get at other applications or services in your system. To minimize access at this layer, consider the following:

- Remove any unnecessary services or programs.
- Don't run LDAP on the same host with other services which are insecure.
- Follow guidance to securely install and configure the web server. The secure configuration of the web server, itself, is critical to securing the host and directory.
- Remove any sample code that has installed as default during the installation of the web server or LDAP directory server. Many of these sample files have been found to allow a system to be compromised.
- Isolate elements of the computer file store from the network. If possible, store the LDAP configuration directory on a separate host from the data directory. This can be helpful in mitigating the risk of backdoor access.
- Use replication. This can provide failover in case of a DoS attack against a specific IP address. Remember, however, that replication is also not yet standardized, and synchronization can become an issue.
- Limit the administrator rights to the server.
- Protect administrator accounts with good passwords.
- Protect, back up, and secure the backup of the Key-Pair file.

Data Layer

The third layer of security to consider is the data layer, which answers the question "What may be done to the information that is accessed?" This is usually controlled at the application level and by using access control information. Here are some guidelines:

- Do not use LDAP to authenticate clear-text passwords. Use hashed passwords.
- Consider using a subset of data replication. This can limit the information available in a less secure way. For instance, if part of your directory is public and part private, you may want to replicate only the public information to a directory instance in the DMZ or outside of the firewall.
- Use SSL with certificates between the application and LDAP directory.
- If the data is very sensitive, use PKI for the clients, as well. (See section below.)
- Consider using an LDAP proxy dedicated to authentication (perhaps a single sign-on product) as an alternative to using private keys for clients if that is not possible.
- Prevent clients from caching SSL files. This can be done by adding the following line inside the <HEAD> section of a file in HTML: <meta http-equiv="pragma" content="no-cache">
- When possible, Run directories as single-application kernel-only machines that fail to a halt. It is better to lose access to the data than to risk the data’s integrity.
- LDIF (LDAP Data Interchange Format) files are used to transfer data between directories or import information into a directory. Since an LDIF file contains information from the directory, these files should be securely protected, as well. To reduce the risk of backdoor access, do not store these files on the same host as the directory.
- LDIF does not provide any method for carrying authentication information with an LDIF file, so the integrity of any files received from external sources must be verified.

Securing Channels Between Servers

LDAP is a client-server protocol. There is no server-to-server protocol, yet. So, use certificate-based authentication between servers. Use SSL to establish the secure tunnel between the LDAP host and application host or between LDAP hosts (replication.)

Many of the currently available LDAP products allow the implementation of replication over SSL. However most do not duplicate ACL information during the replication. This could result in an insecure instance of a directory. If access control is important in the specific implementation of the directory, make sure the ACL information is duplicated.

Securing Channels Between Server and Client

There are a few methods that can be used for secure transport of information between client and server. Encryption can be used for data privacy, checksums can be used to protect data from modification, and passing security tokens can be helpful in authentication.

Most LDAP servers support SSL for encrypted communication. Many also support PKCS#11 APIs for communication with software or hardware modules. A server can verify if a client certificate is valid and from a trusted CA, or can examine information from the certificate and compare it to information in the directory for a user.

SASL can also be used for two-way authentication. It is an internet equivalent of X.509, providing two-way authentication for client-server applications. This mechanism helps a client and an application securely authenticate each other, but does not provide data integrity.

Other Alternatives (XML)

LDAPv3 is primarily an access protocol, and supports static directory information. Some applications, however, require dynamic information.

XML is a content technology designed to transfer data between applications. Thus, for dynamic information transfer, XML becomes an alternative to LDAP. In addition, XML digital signatures can provide for non-repudiation. When used with SSL (to provide confidentiality, integrity, and authentication), XML can increase security.

Because XML is designed to transfer data, it is inherently more flexible than the static, hierarchical model in LDAP. Not all of the information must be moved into a single directory. XML can move or query data from different directory applications, creating a virtual directory or sorts. Thus, LDAP may be augmented by XML to accommodate greater complexity. The security ramifications of the use of XML must also then be considered, but that is for another paper.

Summary

- Secure your network and hosts properly. Because directories centralize information, more expensive safeguards may be justified. Don’t rely on "security by obscurity."
- If your directory is not public outside of your network, make sure it is protected within the firewall.
- Consider using a proxy directory in the DMZ with public information only if this is an option.
- Store configuration data and LDIF files on separate hosts from the directory.
- If you use passwords for authentication, do not store them in clear-text, but use the hashed version.
- If users must authenticate to the directory, implement SSLv3.0 to encrypt the transfer of the passwords.
- Use ACLs to control access to entries in the directory.
- Even if the information in the directory is available to anonymous readers, use ACLs to control write access to the data.
- Consider the use of XML if dynamic directory information is needed. However, make sure

you understand how to secure that.
- Protect passwords and private keys! To quote Gary Flynn of James Madison University, "Of course, with any common authenticator, we have the problem of one password (or private key) providing the keys to all participating applications. Thus user password and key handling becomes a paramount concern regardless of the underlying authentication architecture."

Acronyms:

ACL - Access Control List

PKI - Public Key Infrastructure

SASL - Simple Authentication Security Level

SSL - Secure Sockets Layer

LDAP - Lightweight Directory Access Protocol

LDIF - LDAP Data Interchange Format

VPN - Virtual Private Network

XML - Extensible Markup Language

Howes, Tim, "LDAP: Use as Directed," 1 February 1999. URL: http://www.networkmagazine.com/article/DCM20000502S0039 (3 July 2001).

References

i. Brand, Louis R., "Overview & Security Aspects of the Lightweight Directory Access Protocol (LDAP)," 17 April 2001. URL: http://www.sans.org/infosecFAQ/authentic/LDAP.htm (28 June 2001).

ii. Hodges, Jeff, "LDAP Directory Services: Security," 11 August 1999. URL: http://www.stanford.edu/~hodges/talks/WebSec99/DirectoryServiceSecurity-1999-08-11/sld024.htm (30 June 2001)

iii. Tidwell, Doug, "The XML Security Suite: Increasing the security of e-business," April 2000. URL: http://www-106.ibm.com/developerworks/library/xmlsecuritysuite/ (30 June 2001).

iv. Ibid.

v. Flynn, Gary Flynn, "Re: [unisog] LDAP and security (was: LDAP)," 8 May 2001. URL: http://www.theorygroup.com/Archive/Unisog/2001/msg00787.html (28 June 2001).

Other References:

Bialaski, Tom. "Directory Server Security," Sun BluePrints. December 2000. URL: http://www.sun.com/software/solutions/blueprints/1200/ldap-security.pdf (30 June 2001).

CERT, "Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP)," Advisory CA-2001-18. 16 July 2001. URL: http://www.cert.org/advisories/CA-2001-18.html (24 July 2001).

Good, G. "The LDAP Data Interchange Format (LDIF) – Technical Specification." Network Working Group Request for Comments: 2849. June 2000. URL: ftp://ftp.isi.edu/in-notes/rfc2849.txt (24 July 2001).

Goodman, David, and Robbins, Colin, "LDAP- Moving Forward Frequently Asked Questions," 26 July 2000. URL: http://www.nexor.com/info/LDAP-FAQ-23.htm (30 June 2001).

Goodman, David, and Robbins, Colin, "LDAP- Moving Forward RFCs & Internet Drafts." 8 September 2000. URL: http://www.nexor.com/info/LDAP-RFCs.htm (3 July 2001).

Goodman, David, and Robbins, Colin, "LDAP- Moving Forward LDAP Business Applications and Scenarios." 20 September 2000. URL: http://www.nexor.com/info/LDAP-Apps/LDAP-Apps.htm (30 June 2001).

Howes, Timothy A., Smith, Mark S., Good, Gordon S., Understanding and Deploying LDAP Directory Services, New Riders Publishing, 1999.

iPlanet, "Chapter 5 Working with Server Security," Administrator's Guide. Copyright 2000. URL: http://docs.iplanet.com/docs/manuals/enterprise/41/ag/esecurty.htm (30 June 2001).

Keys, Botzum, "Enterprise Application Security," IBM AIM Services, 17 September 2000. URL: http://www.transarc.ibm.com/~keys/documents/EnterpriseApplicationSecurity.PDF (30 June 2001).

Lewis, Jamie. "Longtime Directory Standards Alone Can't Support E-Biz Apps," InternetWeek.com. 23 May 2001. URL: http://www.internetweek.com/columns01/lewis052301.htm (28 June 2001).

Wilcox, Mark, Implementing LDAP, Wrox Press, Inc., 1999.

Wilcox, Mark, "Protecting Data Over the Wire," The LDAP Heavyweight. May 1999. URL: http://developer.iplanet.com/viewsource/wilcox_protect/wilcox_protect_p.html (30 June 2001).

Wilcox, Mark, "Straight Talk About Security for System Administrators," The LDAP Heavyweight. November 1999. URL: http://developer.iplanet.com/viewsource/wilcox_security_p.html (30 June 2001).