

NEXOR

Security Solutions for a High Assurance Directory Environment

A NEXOR White Paper

July 1999

NEXOR's products provide high assurance messaging and directory solutions. This technical paper how NEXOR's range of COTS products can be applied to provide secure solutions to high assurance directory environments.

For more information, please contact:

Europe

NEXOR
Rutherford House
Nottingham Science & Technology Park
University Boulevard
Nottingham, NG7 2PZ, UK

Phone: +44 115 952 0500

North America

NEXOR
7799 Leesburg Pike
Suite 900n, Falls Church
VA 22043

Phone: (703) 847 8290

Internet: www.nexor.com

Email: info@nexor.com

Contents

1 INTRODUCTION.....	3
2 ACCESS CONTROL.....	5
3 AUTHENTICATION.....	6
3.1 NEXOR's Strong Authentication Solution.....	6
4 ISOLATED DIRECTORY.....	8
5 DIRECTORY FIREWALLS.....	9
6 DATA REPLICATION.....	10
7 SUMMARY.....	11
ABOUT NEXOR.....	12
ABOUT THE AUTHOR.....	12

No warranties or guarantees, expressed or implied, are given. In no event will NEXOR or any person acting on behalf of NEXOR be held responsible for any consequential, incidental or indirect damages (including damages for loss of business profits, business interruption, loss of business information and the like) which can be claimed directly or indirectly to be a result of taking any action as a result of the contents of this document.

1 Introduction.

Directory services, today, are a fundamental component of the network communications architecture. The directory is being used to hold anything from user based white pages information such as phone numbers and email addresses, to operating system information such as the application access privileges and network routing information.

By holding such diverse and critical information, the directory has become a fundamental infrastructure component of a business. If an attacker can alter the directory, the day-to-day operations of the business can be significantly interrupted.

As an example, let's assume you want to send an email containing an invoice for "services rendered" to the President of the United States, but you do not know the email address. You might use the US Government Online Directory (GOLD), and search for the term "president". In most integrated messaging and directory system the result of such a search would be put automatically into the "To:" line of your email message. In most cases what the user will see is a shortened "name" in the "To:" address line and not the detailed address information. If this directory was not secure, a subversive/hacker could modify the directory entry for the President and substitute the underlying email address with "hilary@whitehouse.gov". The unsuspecting user would send her email and invoice to the wrong person – and who knows what the consequences of that could be!

To get back to basics, in networking terms, directories are typically accessed using the Lightweight Directory Access Protocol. LDAP is defined by the Internet standards community, and provides a mechanism for passing text-based requests for information from a client (desktop machine) to a directory server. Its aim is to let users quickly and easily query directories for information - for example user names, email address, and/or telephone numbers. These inquiries can be made secure with existing technology (such as SSL and TLS services) as long as the information requested is on the server to which you are connected.

In many cases the information that you are searching for may not be on the server that you are connected to. LDAP, as the standard exists today, does not define how different servers, especially as implemented by different vendors, cooperate to provide a distributed service (such as the US GOLD Directory). This leaves the door open for security attacks. This paper examines how such attacks can occur, and how they can be protected against.

2 Access Control

The first level of defense in a directory system is what is called access control. This is a software mechanism employed by the directory to ensure that each LDAP request is only able to access the data that the end user is authorized to see.

Standards based access control is vital in a distributed environment, particularly in heterogeneous environments. In distributed environments, to increase efficiency and robustness of the solution and conserve network bandwidth, certain elements of the data are normally replicated or cached by multiple servers. If the directory server holding the copy information is not fully aware of the access controls deployed by the server holding the original information, there is a danger the copied information could be revealed to unauthorized users or hackers.

This is one of the main dangers of an LDAP based approach to directory services. The LDAP model does not define¹ procedures for distributed operations or an access control model, requiring security measures to be implemented outside of the main directory data servers (for a further discussion of this, see Section 5 which discusses directory firewall technology).

NEXOR Directory provides a full distributed access control mechanism with its implementation of the X.500² (93) standards based directory, providing what are called “simple” and the more complex “basic” access controls.

The X.500 Access Control Information (ACI) model comprehensively defines access to information within the directory server. Such controls are configurable and highly flexible within NEXOR Directory, enabling the system administrator to control access for specific groups, individuals or even applications. For example, access rights can be granted to all employees for certain information – everyone’s e-mail address and office phone number for example. Certain groups - Human Resources, lets say – can be given access to payroll information. Another example of access controls might be at the individual level where each employee can change his own home address. Not only the types of information that may be accessed, but also read only and write permissions can also be configured.

3 Authentication

Authentication is an important concept for directories, and is closely associated with access control. The X.500 based NEXOR Directory access control mechanisms define who can access the directory, which items of data can be accessed, and what can be done with that data (e.g., read or modify). To perform this level of access control the directory needs to know who it is that is accessing the data – this is where authentication comes in. Authentication is the mechanism used by the directory server to identify and validate the accessing end user.

There are three levels of authentication a typical directory can implement:

- **None** – The user connects anonymously, or provides a name that cannot be verified. This is typically used to access a public directory service where user identification is not important.
- **Simple** – The user needs to provide a password to verify their identity. The password can be in clear text or hashed¹. This may be used within a corporation by an individual to change their home address.
- **Strong** – Digital signature and cryptographic security techniques are used to provide a high level of assurance as to the identity of the user. This is rarely used today except in very high assurance environments such as military, intelligence and financial services environments.

Most products offer the first two levels of security, but only a few offer a comprehensive strongly authenticated solution.

3.1 NEXOR's Strong Authentication Solution

To provide strong authentication, NEXOR has chosen to implement a standard known as SDN 705². SDN 705 is a detailed implementation guide defining precisely how digital signature techniques should be used to provide a secure *distributed* directory under the X.500 protocols. SDN 705 has been initially proposed for applications in the US Military and Intelligence communities where high assurance is critical to the security of the nation.

¹ Hashing is rarely used, as the distributed operation is complex and not defined by the standards.

² Secure Data Network System developed under the sponsorship of the NSA.

Digital signatures are used in X.500 in two different ways:

- They are used to provide client-to-server and server-to-server authentication. The earlier strong authentication examples show this use.
- They are used to sign the actual directory operations. This provides an additional level of assurance as information requests are passed from server to server in a distributed directory.

Distributed is a key point. Many products are able to offer secure LDAP access to the directory. This secures the client-to- (initial) server protocol, but does not offer an end-to-end solution. Server-to-server traffic also needs to be authenticated. To provide a distributed solution you need a distribution protocol such as the X.500 Directory Server Protocol (DSP), which is able to encapsulate the end user query and results within the server-to-server communication data stream. This data stream can then be authenticated as it moves from server-to-server.

(SDN 705 also defines other key elements of a directory security system, such as how to avoid deadlocks... Digital signature technology relies on public keys. These keys are stored in the directory. If the directory itself uses public keys, unless care is taken, you cannot start secure operations until you access the directory, but you cannot access the directory until you have secure operations – so you get locked out.)

4 Isolated Directory

While the protocols can be protected using some of the mechanisms described in this paper, there are other ways to attack the system. A second level security threat associated with directories is *back door access*.

A directory uses a database to store its information. At some point this information is then stored on the computers disk. This disk database could be accessed directly by an attacker using a file transfer program or by a directly logging into the computer itself from a network. This completely bypasses the directory access control and protocol security mechanisms.

NEXOR is currently researching running the directory on what are being called “trusted” operating systems. These provide a separation between the network and database; thereby ensuring the only access to the database is from the (already secured) directory protocols.

5 Directory Firewalls

Directory systems are presenting a security paradox to organizations. On one hand, more and more information is being added to the directory for *internal* use – for example home telephone number of all employees. This information is for internal use only, and in most cases you do not want to publish it. However, the same directory system, and even the same directory entries, contains public key security material that needs to be published widely to facilitate secure messaging and e-commerce.

The traditional solution to this is access control. But more and more directory systems are no longer single vendor solutions, but a mesh of different, loosely coupled, directory systems – the so called *meta-directory*. Access control cannot be relied upon in these environments, as there are few standards, and different systems implement different solutions.

NEXOR has developed a solution called the NEXOR *Directory Boundary Agent* (DBA)³ to resolve this. The DBA is an application level firewall designed to mediate between the internal and external directory requirements. In the example above, it can allow access to public key information but protect home phone numbers. It, however, goes further in that it doesn't just tell the inquirer that they don't have access to the information – it denies the existence of the requested information. Telling a hacker that he can't access information is very different from responding that you don't know what he is talking about!

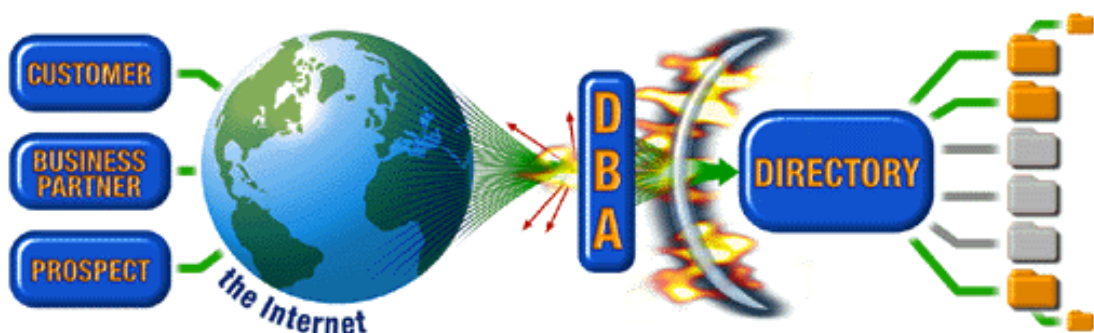


Figure 1 NEXOR Directory Boundary Agent

³ This product incorporates TABARDIUM® technology. TABARDIUM is a registered trademark of the UK Defence Evaluation and Research Agency (DERA).

6 Data Replication

To provide for robustness and efficiency in a distributed directory, it is common practice to replicate the data between servers. A NEXOR white paper "Reliability in a High Assurance Directory Environment" looks in detail at what this entails, and the strategies that can be deployed.

If data is to be replicated, the replication mechanism itself has to be secured. NEXOR is one of the few vendors able to offer solutions in this area.

First, the digital signature techniques discussed in Section 3 (above) can also be applied to the X.500 protocol for replicating entries between servers - Directory Information Shadowing Protocol (DISP). This ensures the data being copied from one server to another cannot be altered by an attacking system.

Second, the Directory Firewall technology discussed in Section 5 (above) has been extended to cover the DISP protocol. This allows a directory system to be configured that has both public and private information – allowing the public information to be copied outside the secure domain to less or unsecured environments. The Directory Firewall can be used to ensure that confidential data is not replicated between the secure and unsecured systems

7 Summary

For NEXOR's customers, the directory represents a key component of a high assurance messaging architecture. This paper examined some of the security issues associated with directory services. It outlines the key concepts used to secure these directories, and presents the solutions NEXOR's products offer.

NEXOR is confident that with these security solutions we can meet the most demanding directory requirements.

About NEXOR

Formed in 1990, NEXOR, the premier defense messaging provider, delivers mission-critical solutions to business and government organizations demanding a robust, secure and scalable messaging infrastructure. NEXOR range of high-performance messaging and directory products meets the industry standards and conformance criteria demanded by the US and Canadian defense forces, the UK Ministry of Defence as well as similar high profile organizations.

NEXOR products are used as the reference platform against which other standards-based products are measured by the UK's National Computing Centre in Manchester and the US Department of Defense, Joint Interoperability Test Center. More information on NEXOR can be found at the NEXOR Web site located at www.nexor.com.

About the Author

Colin Robbins, NEXOR's Product Strategist, is responsible for the direction of NEXOR's solutions, which includes identifying new markets for products and developing strategic technology and channel partnerships. Robbins' has provided consultancy on an International basis in all aspects of pragmatic security, messaging and directory deployment.