
DataDirect Connect[®]

Data Access Middleware Security Simplifies Business Process Applications

Internet Security Advisors Group



About Internet Security Advisors Group (ISAG)

The Internet Security Advisors Group (ISAG) is an international information security firm specializing in mass marketing product security offerings through channel partners. Ira Winkler, one of the country's most highly regarded experts in corporate and computer security, founded ISAG in 1997.

ISAG is a world leader in the performance of security services such as vulnerability assessments, penetration testing, policy development, product implementation, and security architecture development and review. Our security engineers are extremely familiar with all methods used by hackers and criminals. We know how hackers probe systems covertly without being detected and how they actually commit their actions and cover their tracks. All efforts performed by our engineers are bonded and several hold current DoD security clearances. A summary of the breadth of skills that our security engineers possess follows:

- Firewall implementation
- VPN & Encryption implementation
- Intrusion Detection System planning and deployment
- Authentication Services implementation
- Web Application Security techniques
- Operating System Hardening
- 24X7 Managed Security/ Incident response
- Vulnerability assessments
- Penetration testing
- Security policy development and planning
- Security Architecture Review and Development
- Code reviews
- Customized solutions

DataDirect Connect[®] Data Access Middleware Security Simplifies Business Process Applications

Introduction

The Internet Security Advisors Group reviewed the architecture and functionality of the DataDirect Connect product line of standards-based data access components offered by DataDirect[®] Technologies. The DataDirect Connect products provide high performance access to a wide range of relational databases through standard ODBC, JDBC[™] and ADO.NET interfaces. DataDirect Connect also incorporates a variety of security features including Kerberos authentication and Secure Socket Layer (SSL) data encryption.

DataDirect Technologies, an independent operating unit of Progress Software, sought to independently verify design and implementation of the security features. The Internet Security Advisors Group has a wealth of experience in reviewing application security, advising product developers and investigating security compromises. Based on our independent assessment, we believe that using DataDirect Connect for database access is one of the best proactive security measures an organization can take to reduce security related losses.

The DataDirect Connect product line is one of several options that can be used for data access. Unlike other alternatives, DataDirect Connect provides ubiquitous data access security for applications by including comprehensive support for a variety of security protocols. The Internet Security Advisors Group praises DataDirect for proactively providing their customers with security functionality, instead of forcing customers to purchase additional products. By doing so, DataDirect prevents development risks for customers that rely on other options.

The security capabilities provided by DataDirect Connect could have prevented many recent and highly publicized security incidents, including the one in which criminals stole more than 45 million credit card numbers, costing T.J. Maxx more than \$150,000,000. The security capabilities of DataDirect Connect are directly relevant to applications deployed in today's demanding IT environments.

While the Internet Security Advisor's review did not include a line-by-line code review, we did conduct an architectural review that verified the design, development and testing of DataDirect Connect. The product line is widely used in corporate environments to support custom application development initiatives. The fact that DataDirect Connect is embedded by over 300 software vendors proves that DataDirect Connect addresses the potential security vulnerability inherent in database access software product.

Security factors are not only a technical consideration. Robust security can also be a critical business enabler. As Web 2.0 and other data and application frameworks are implemented, security must be a fundamental design concern.

Organizations that use DataDirect Connect to develop their distributed applications simplify development, and automatically include data encryption and authentication in their applications. By choosing DataDirect Connect, organizations ensure that their applications will realize the documented benefits of high performance and interoperable data access. They also are providing a solid security foundation. Because of this combination of factors, particularly the security features, the Internet Security Advisors Group strongly recommends that organizations consider DataDirect for their database access middleware needs.

Application Security and DataDirect Connect®

Many people understand the need for application security. The value of securely authenticating users and protecting data transmitted over a network in a distributed application environment is obvious. But it may not be clear how security relates to a data access interface such as ODBC, JDBC™ and ADO.NET. Actually, security plays a critical role because these data access middleware technologies control every aspect of communication between the application and the database. The middleware components are responsible for establishing and managing connections from the application to the database, sending requests from the application to the database, and then transmitting data from the database back to the application.

Some common tasks performed by the middleware include:

- Connection and statement pooling
- Connection failover and load balancing
- Data conversions between database and standard API specification
- Meta-data support
- Internationalization and code page support
- Thread management
- Data caching
- Buffering
- Throughput socket management

Today's applications leverage many different application topologies. In some cases, the application is running on a desktop client and connecting over the network to a database. In other cases, an application is hosted on a middle-tier server and connects to a database running on another set of servers. Other application topology factors to consider include whether the application is running on an intranet or the public Internet, and the degree of physical distribution. To meet the needs of distributed organizations, applications are often not limited to internal usage. Rather, they are highly distributed, resulting in the wide distribution of data and application usage. Given the critical role of the database middleware access layer, it is important that the middleware be implemented securely, and that it provides the security capabilities needed for distributed applications.

To meet these fundamental application needs, the data access middleware must provide robust mechanisms for authentication and data encryption. A wise foundation for application security includes Kerberos for authentication, Directory Services for authorization, and SSL to protect data in transit. Although many developers expect that the middleware providers will supply such functionality, it is usually not integrated into products by the vendors. DataDirect Technologies includes these security options as standard features in their DataDirect Connect product line, making it easy to provide robust application security in a way that is easy to maintain.

What is Data Security?

Security professionals traditionally define data security as Confidentiality, Integrity and Availability. With regard to middleware, data is secure when the sender and receiver are confident that all the data was transmitted correctly and that access to the data is restricted to the intended parties. Data security reduces business risk, but does not eliminate it.

Businesses need to secure data for a wide variety of reasons. Some of these reasons are obvious, such as the protection of proprietary information. Organizations are increasingly called upon to protect data relating to their business partners and customers. If an organization needs to scale their business by working with business partners, it is important to secure information in transit, information that will cross multiple business boundaries. Security of information transferred between users and applications also facilitates applications that would not otherwise be possible. Data security included in middleware makes businesses more versatile, and inevitably more profitable.

Even companies that don't treat their databases as a competitive advantage realize that the compromise of their databases can lead to disaster, exposing an organization to huge financial losses. The infamous T.J. Maxx credit card incident resulted in the loss of more than \$150,000,000, and there are hundreds of similar incidents in recent years. In the current business environment, a security compromise often results in loss of customer trust and the potential for huge financial liability.

Security is essentially about effective risk reduction. Effective risk reduction means that your security approach does not depend on a single point of protection, such as a firewall. Effective risk reduction requires a layered approach to security that addresses the many ways that data can be compromised. With criminals increasing their efforts on targeting any computer-based information that has value, enterprise IT departments are well served to closely examine all effective methods to reduce risk of data loss or compromise.

As witnessed by the T.J. Maxx incident, one of the most costly security losses is when an intruder is able to gain access to a trusted network and monitor data transmissions. If intruders succeed in making unauthorized computers appear to be authorized and trusted, they can gain long-term access to a network with potentially devastating results.

The DataDirect Connect product line helps to secure a company's information assets by enforcing authorization control and by protecting data that is transmitted across the network. Secure and reliable authentication limits the chance of authorization errors, preventing outsiders and unauthorized insiders from gaining access to your network or trusted applications. The DataDirect Connect product line protects data in transit by providing the ability to encrypt database information between the application and the database. Because organizations can use this capability to stop internal and external users from eavesdropping on sensitive information, companies can confidently develop business relationships and share information across the Internet with safety.

Today, multi-tiered applications are the norm as developers have moved to segregate functional responsibilities into discrete components or layers. This progression has led to more efficient development patterns, but it complicates factors that must span multiple layers, such as logging and security. While Aspect Oriented Programming (AOP) provides a programming paradigm that helps manage cross-cutting concerns related to application layers, Kerberos provides a standards-based mechanism for secure authentication. Kerberos includes the ability to support user delegation. Delegation of authority means that a user interface acts on behalf of the user while manipulating business objects.

One of the big failures of Java RMI, SOAP, SAML and other programming standards is the fact that they make no provision for delegation of authority. Without delegation of authority, developers must fall back on custom solutions, creating proprietary, brittle architectures that require constant updating at great expense. Only Kerberos allows for the development of secure, scalable and robust multi-tiered applications. DataDirect Connect provides the most consistent Kerberos-enabled data access middleware implementation on the market.

What is Single Sign-On (SSO)?

Traditionally, good security procedures require that a password is not reused across multiple applications. Should a password be compromised, all systems and applications using the same password would be compromised. Users have been forced to create and store or remember increasingly numerous passwords in their business and professional lives. Single Sign-On (SSO) eliminates the need for multiple application passwords. Instead of multiple accounts using the same password, SSO manages account credentials across all applications on behalf of the user.

SSO significantly reduces the likelihood that accounts can be compromised. In addition, it reduces IT operations costs associated with password resets. Just as important, SSO allows organizations to easily recover and manage user information, such as the departure of personnel from an organization, or to constrain an individual involved in a security incident.

For an application to participate in SSO, all the components or layers in the application, including the database access middleware, must work together to enable SSO. Kerberos is now accepted as the preferred approach for implementing an authentication process that supports SSO.

Meeting Regulatory Requirements

Organizations must comply with a sea of regulations. While existing regulations are rarely eliminated, new regulations appear regularly, and many regulations are vague in defining precisely how an organization can achieve compliance.

Regulatory requirements consistently demand data protection and user authentication. DataDirect Connect and Aspect Oriented Programming are ideal solutions to satisfy a wide variety of current and future regulatory requirements and should be considered critical components of any security program.

Managing Application Development Risks

When you introduce a middleware layer into network architecture, you increase risk in the development effort. This risk is offset by the reward of reduction in other development, operations, and maintenance risks. The DataDirect Connect product line protects applications from being bound to a specific database vendor by using a common set of standards-based APIs such as ODBC, JDBC™, and ADO.NET. DataDirect Connect provides interoperable interfaces. These interfaces eliminate the need to recode software for different platforms and database management systems, increasing an application's portability, reliability and longevity.

A Firewall is Not Sufficient

When it comes to security and risk, many developers believe that keeping intruders out of the network is sufficient for addressing security requirements. Firewalls and perimeter security in general are a critical part of any security program. However, they address only a portion of necessary security requirements.

The infamous T.J. Maxx credit card thefts were accomplished because someone compromised the company's perimeter. While some firewalls have integrated VPN functionality that might provide some encryption capability, this encryption will not address data that is transferred to a non-homogenous system. Likewise, it does not protect data that is being transferred within an organization.

In addition, firewalls do not perform Identity Management. Therefore they do not provide authentication for systems and applications that run within a network. Firewalls alone do not address the regulatory requirements specific to Identity Management.

Service Oriented Architecture (SOA)

More and more organizations are moving to Service Oriented Architectures (SOA) to improve the flexibility and agility of their IT efforts. In many cases, data services and data access layers are integral foundation technologies for SOA initiatives. These technologies provide consistent access to underlying heterogeneous data sources. Because many applications and Web services share a common data service or data access layer, it is critical that the architecture is both secure and scalable. Data services that use DataDirect Connect products benefit from built-in security features such as Kerberos and SSL.

Identity Management is the Bedrock of Rights Management

Data and applications are typically deployed in heterogeneous environments. Rights management for applications must address the fact that data often spans a wide variety of applications, firewalls, operating systems, database management systems and so on. Implementing rights management can be extremely difficult without an integrated Identity Management framework.

When different systems have their own Identity Management frameworks, asserting uniform rights management is difficult. The Identity Management implementation in DataDirect Connect relies on industry-standard Kerberos, which is available on most platforms. Kerberos enables the operation of a single Identity Management system. Rights management can be deployed in several ways, one of which is the use of Aspect Oriented Programming or AOP. AOP can be implemented at either compile time or runtime. Using runtime AOP is easy in managed code environments like .NET and Java, but AOP is more difficult in a C or C++ environment. The advantage of using AOP is that it provides the ability to implement a policy regarding all executable objects.

OS Authentication and Single Sign-On

Introduction to Kerberos and NTLM

Kerberos has been the default method of authentication for Microsoft Windows® for some time, displacing the earlier NT LAN Manager (NTLM) protocol. Kerberos was chosen because it was widely used and secure. NTLM, on the other hand, is a proprietary technology that has questionable security value. Many database drivers, such as those for Microsoft SQL Server 2005 revert to NTLM silently when an application spans domains. It is important to ensure that the authentication mechanism does not revert to NTLM silently, because this may present grave security consequences.

The remainder of this document will be focused on Kerberos because it has become the de-facto standard and it is more secure than NTLM. Also known as RFC 4537, Kerberos was created by MIT in the 1980s and has since been adopted as the standard mechanism by Microsoft (as of Windows 2000), which now supports GSS-API (RFC 1964).

Kerberos takes its name from the three-headed gatekeeper of the underworld in Greek mythology and has three essential parts:

- A client, which can be a process or a user
- An authorization server referred to as a Key Distribution Center (KDC)
- A service provider such as a database, Web server, or other n-tiered business service

Kerberos is built on the principle of third-party trust. The client and service provider uses a mutually trusted KDC to establish a trusted relationship. We will focus here on a few key elements to illustrate the underlying mechanism.

When an application client wants to access a particular service, such as a relational database, it must request that service from a provider. To establish a trust relationship, both the application client and database service provider need some assurance that the other entity is not a hacker impersonating a legitimate entity. They establish this trusted relationship by using a trusted third-party KDC.

For the moment, we will focus on Authentication and Identity Management. Kerberos has little to do with the authorization a particular user has, but will supply a list the administrator creates to other authorized entities. Kerberos is an Identity Management and data security tool more than an authorization mechanism. Microsoft Windows supplies the authorizations through Active

Directory, thereby providing the necessary complement to Kerberos.

The client gets a ticket for the service from the KDC and the server verifies it before proceeding. The client, on the other hand, verifies the server to ensure the server is not spoofed. This is also done with the help of the KDC. No passwords are sent over the network, but rather hashed values of secret data that only the client, KDC, or service provider could know. This information is stored in an encrypted header and each party is responsible for decrypting and verifying the information it needs. Some of the data from the KDC is encrypted with a password that only the KDC knows. When messages are sent to it from other sources, it can open this section to check for tampering and authenticity, so it is not possible to subvert the KDC, or other entity, by manipulating the packet contents.

Note, however, that tickets expire. Privileged tickets, such as those with the instance "root", expire in a few minutes. Tickets that carry more ordinary privileges may be good for several hours or a day, depending on the installation's policy. If your login session extends beyond the time limit, you will have to re-authenticate yourself to Kerberos to get new tickets.

Kerberos provides authentication and message integrity (KRB_SAFE) encryption (KRB_PRIV). In addition to superior security, Kerberos has two other advantages over NTLM; it is faster and provides for delegation. It is faster because the protocol is simpler than NTLM in that it requires fewer trips to the server. It provides delegation by allowing users to signify that a service may act on their behalf.

Microsoft SSPI vs. GSS Standard Kerberos

Most Microsoft extensions have been incorporated into RFC 4757. Sun's Java SE 6.0 provides the industry's most functional Kerberos/GSS implementation. Kerberos supports the encryption of packets using AES-128 (AES-256 with JCE crypto policy), RC4-HMAC (from Microsoft), 3DES CBC-SHA1, DES-CBC-CRC, or DEX-CBC-MD5.

Kerberos also supports IPv6. Native GSS-API support exists for UNIX, Linux, Mac OS X and Microsoft Windows (via KfW and SSPI). Major Kerberos implementations include MIT Heimdal and the Sun Java distribution. In general, companies would be well advised to get expert help in setting up Kerberos.

Kerberos Features Overview

Delegation of Credentials

Relative to database connectivity and Kerberos, there may be times when you want the application to use the credentials of the actual end user (vs. the user-id associated with the machine that is executing the application) when connecting to and authenticating with the database. Kerberos supports this capability by delegating the credentials associated with the end user so that those credentials can be used for database authentication.

Kerberos provides for delegation by allowing the application code to set the "forwardable" flag, and by allowing only designated servers to be configured to perform operations on behalf of the original client. Other competing technologies are required to get the original user's certificate, which could result in a security breach that should be avoided at all cost. Alternatively, the service provider can act on its own authority and note the actual user via a logging mechanism.

In this latter scheme, the original user's identity is destroyed or altered. This makes building a multi-tiered application inherently insecure, beyond the usual problems arising from poor coding, legacy requirements and so on. In other words, non-Kerberos systems are inherently flawed or are proprietary and limited in use.

Kerberos also supports the ability to transfer trust between domains or realms. The realms must have an established trust relationship. Windows sets up this trust relationship within a tree or forest by establishing trust relations with domain controllers one level up and down from any other controller.

Establishing trust between forests is difficult and must be attempted only after gaining considerable experience. One method is to recognize a KDC from another organization as the Ticket Granting Server. Then the user gets a ticket to get that server for access to services in the other domain. Once they are in possession of an external domain's ticket for services, they can request services from the other domain. Trust is transitive: if Alice trusts Bob, and Bob trusts Carroll then Alice will trust Carroll. This may or may not be the intent. Modifying this behavior requires source code changes.

Reauthentication

Reauthentication is unique to DataDirect Connect. It is useful when using a connection pool to provide scalable connections. Re-Authentication effectively creates a shared resource pool. Some implementations of Kerberos want to reissue a ticket for each access. Although this is normal practice, doing so may seriously degrade performance if a re-authentication request is generated for every URL. DataDirect Connect caches authentications and if another request is made when an object is already in the pool, that object gets reused. This modification substantially improves performance.

Summary: Kerberos Authentication and SSO

The DataDirect Connect approach to database driver middleware supports Kerberos to securely authenticate user access from the application to the relational database. This is important regardless of whether your application leverages a client-server or multi-tier network architecture topology. DataDirect supports SSO and optionally, delegation and re-authentication, without demanding novel features of the operating environment or additional application code.

Given the broad level of support for Kerberos on Windows, UNIX and Linux platforms as well as in databases such as Microsoft SQL Server, Oracle, DB2 and Sybase ASE, this approach gives the consumer a transparent middleware solution with good support and performance.

Delegation is absolutely critical when leveraging a grid-based architecture where multiple CPUs can service various parts of the same request. Grid architecture is scalable and supports many functions necessary for multimedia-rich transactions. For example, complex renderings and mashups run faster when using multi-threaded tracing rather than serial raster image manipulation. It is critical that the application middleware can authenticate and properly delegate credentials to the various computing resources in a grid environment.

Data Encryption

Introduction to Encryption and SSL

The SSL protocol is a well established mechanism for establishing secure data transport. Although it is primarily used when two parties do not know each other, SSL can be used in an application scenario where the design does not rely on symmetric key lists. In an Internet environment, it leverages the open standard HTTPS port, as opposed to the Kerberos port (88), which is generally closed.

An SSL session starts with a public key handshake where the certificate of the user and server are examined by each other. If the keys, timestamps, and authorizations are complete, a symmetric key such as that used for DES or AES is exchanged. The session is then encrypted using this key.

SSL does have the concept of a virtual user, but does not have delegation. This fact is crucial when allocating operating system resources to implement security. With delegation, the operating system is involved in protecting the object in a manner consistent with policy. With virtual users, the application is in charge of implementing policy. Even if there are no coding errors, the complexity of maintaining such a system is daunting.

SSL Features Overview

SSL uses Public Key Interchange (PKI) to provide authentication between parties, where one or both parties can actually be services running on a computer. Each party has a two-part key. One part is a public key that is distributed directly or through a database such as LDAP. The other part of the key is always private and is never used by anyone or sent across the network.

SSL supports many encryption standards and has mechanisms for selecting among them based on capabilities, policies, and legal restrictions. SSL supports RSA, Blowfish, SHA, IDEA, DES, Diffie-Helman, Cast RC2/4/5, and AES encryption standards with various numbers of bit length keys.

Since SSL is supported by every Internet browser, it has become the predominant mechanism used to encrypt data that flows between a Web browser and the application/Web server that is serving the application pages. From a database middleware perspective, this paper describes how SSL can be used to encrypt the data between the database server and the application.

Encryption Using DataDirect Connect

Because DataDirect Connect provides integrated support for SSL, applications that leverage DataDirect Connect can choose to have the data that flows between the application and the database encrypted automatically. Doing so significantly reduces the risks associated with the most common industry data thefts.

Although it is possible for developers to implement encryption through other means, DataDirect Connect includes encryption support as part of its core functionality. More importantly, DataDirect Connect encryption relies on development libraries that are both well tested and widely available on all common computer architectures. This approach simplifies the implementation process, reduces the long-term risk of developed applications and architectures, and minimizes the complexity of the development effort.

Conclusion

The DataDirect Connect product line provides ubiquitous security, including support for SSO through Kerberos and data encryption through SSL. The Internet Security Advisors Group believes that these security capabilities make any application developed using the DataDirect Connect products fundamentally more secure than applications employing competing products. Companies are strongly advised to consider DataDirect Connect in the design stage of their application development.

The DataDirect Connect solution is strengthened by the fact that this product line uses standard security protocols that are natively supported by standard computer configurations. An additional proof point relates to the fact that DataDirect Connect technology is well tested and widely used by many corporations and ISVs. This validation of DataDirect Connect minimizes the risks associated with development and deployment efforts.

DataDirect Connect provides a well established data access middleware product line that addresses the functional requirements of implementing business processes. By providing seamless connectivity between heterogeneous clients to heterogeneous relational databases, DataDirect Connect provides a solution that decreases development and operations cost, while allowing for great versatility. By integrating support for security features such as Kerberos and encryption, into their software, DataDirect Connect exponentially increases the security of applications.

As discussed, Kerberos provides Identity Management while keeping rogue systems off of the network. These functions alone can prevent the computer crimes that result in theft of critical information and the damage to personal and organizational reputations, which can be even more costly than data loss. Identity Management means that user credentials can easily be passed around a heterogeneous environment. Without this functionality, users are typically granted too much access, facilitating insider abuse.

Likewise, Kerberos reduces the risk of intruders entering the network because their systems will not be recognized by the network. Even if attackers were able to gain access to a legitimate system, they would need to overcome yet another hurdle to establish credentials on the network.

With the DataDirect Connect product integrated into the applications, the entire transaction is secured. Without DataDirect Connect, a variety of products need to be integrated together or the entire process is performed without any security. You only have to read any recent copy of ComputerWorld or InformationWeek to see the likely results of that.

Using DataDirect Connect products allows you to provide pervasive security across your organization. In total, the DataDirect Connect solution helps organizations reduce or eliminate development, operational, security and regulatory risk. With the provision of this pervasive security, organizations reduce their loss and liability risks. With the growth of computer-based crime and losses, DataDirect Connect must be considered a viable option for all development efforts.

About DataDirect - Industry leading ADO.NET, JDBC™, ODBC Data Connectivity

DataDirect Technologies, an independent operating unit of Progress Software, is the industry's most comprehensive provider of standards-based data connectivity products. DataDirect Connect consists of ODBC drivers, JDBC™ drivers and ADO.NET data providers for all major relational databases such as Oracle, DB2, Microsoft SQL Server, Sybase ASE, and Informix.

DataDirect Connect® for ODBC™

DataDirect Connect for ODBC database driver's unique wire protocol design eliminates the need for database client software and libraries, greatly simplifying installation and deployment, and dramatically improving application performance and scalability.

DataDirect Connect® for JDBC™

DataDirect Connect for JDBC offers the fastest and most comprehensive suite of Type 4 JDBC™ drivers and is the SPECjAppServer/ECPerf performance and scalability leader. This suite supports distributed transactions, connection pooling, updating BLOB/CLOB data types, and Windows authentication.

DataDirect Connect® for ADO.NET™

DataDirect Connect for ADO.NET is the industry's only suite of ADO.NET data providers with a 100% managed architecture, eliminating the need for database clients, boosting performance, and delivering a flexible, secure connection to Oracle, DB2, Sybase, and Microsoft SQL Server.

DataDirect also provides the following products:

DataDirect OpenAccess; a development toolkit for building custom ODBC, JDBC™, ADO.NET, and OLE DB drivers for proprietary data or applications.

DataDirect Shadow® is the industry's only comprehensive platform for mainframe integration providing standards based access to the widest range of mainframe data, applications, and screens. With DataDirect Shadow, customers can gain cost effective, high performance access to the mainframe via standard SQL and SOA interfaces.

DataDirect XQuery® is a high-performance, scalable, embeddable XQuery implementation that plugs easily into any Java architecture and accesses almost any data source without being dependent on underlying servers or proprietary extensions to XQuery.

DataDirect XML Converters™ are high-performance Java components that provide bi-directional, programmatic access to virtually any non-XML file (EDI, flat files, etc.). XML Converters allow developers to seamlessly stream any non-XML data as XML to industry-leading XML processing components or to your own applications.
