Security Features in Teradata Database

By:
Jim Browning and
Adriaan Veldhuisen
Executive Summary

The Teradata® Database supports many important features that are designed to enhance the security of an enterprise data warehouse. These security features include:

> User-level security controls.
> Increased user authentication options.
> Support for security roles.
> Enterprise directory integration.
> Network traffic encryption.
> Auditing and monitoring controls.

This white paper provides an overview of the security features and describes scenarios for their usage. The paper will also discuss the independent evaluation of the Teradata Database to the International Common Criteria for Information Technology Security Evaluation (ISO 15408) standard.
Introduction

Increased public attention to security is driving the restructuring of security requirements. The role that IT will play in helping address these challenges will be significant. However, IT departments are under pressure to cut their operating costs, while being asked to improve and standardize information security. Teradata Corporation’s security approach will assist Teradata Database Security Administrators who are facing these new challenges.

Legislated requirements, government regulations, and industry standards all result in a continually evolving security landscape. Following are examples that are driving increased requirements for data warehouse security across many industries and geographies:

European Union Privacy Directives
The principles established by the European Union (EU) Privacy Directives serve as the foundation for many international privacy and security laws. These directives require the use of appropriate technical and organizational measures to ensure confidentiality and security of processing of personal data.

Health Insurance Portability and Accountability Act
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates standards and requirements for maintaining and transmitting health information that identifies individual patients, and compliance is required by all U.S. health care organizations that maintain or transmit electronic health information. A Security Rule establishes specific security requirements for authorization, authentication, audit trail requirements, secure data storage and transmission, and data integrity.

Gramm-Leach-Bliley Act
The Gramm-Leach-Bliley Act of 1999 (also known as the Financial Modernization Act) requires that financial institutions adopt policies and procedures to provide for the protection of financial information that identifies individual consumers. Such procedures must protect against any anticipated threats or hazards and protect against unauthorized access which could result in substantial harm or inconvenience to a customer.

Sarbanes-Oxley Act
The Sarbanes-Oxley Act of 2003 includes a number of reforms intended to increase corporate responsibility, improve financial disclosures, and protect against corporate and accounting fraud. While this legislation does not mandate the use of specific security controls, Section 302 does require that internal controls be established to protect data from both internal and external threats, and Section 404 requires that corporations report on the effectiveness of those controls. Also, Section 409 requires the disclosure of any material changes to the financial condition or operation of the company (potentially to include a major security compromise).

Personal Information Protection Act (Japan)
The Japanese Personal Information Protection Law requires that companies operating in Japan develop and implement information privacy and security controls for any databases or documents containing consumer or employee information. This obligation will be applied to any party who stores and uses more than 5000 persons’ information in total in the party for its business. Japan's Ministry of Economy Trade and Industry (METI) has issued specific guidelines for maintaining the security of these databases.

Payment Card Industry Data Security Standard
Developed by Visa and MasterCard, the Payment Card Industry Data Security Standard applies to merchants and service providers that store, transmit, or process credit card transactions. The standard outlines 12 specific requirements that must be implemented to protect cardholder information.
Security, as an aspect of IT control requirements, defines an attribute of information systems, and includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability of critical services and, indirectly, privacy. Data in a data warehouse must be protected at both ends of a transaction (user and enterprise). Figure 1 depicts the relationships in simple terms.

These concepts and relationships are taken from the Common Criteria ISO 15408 standard specifying the "Privacy Class of Common Criteria". It proposes that all security specifications and requirements should come from a general security context. This context states that "security is concerned with the protection of assets from threats, where threats are categorized as the potential for abuse of protected assets."

Data warehouse security requires protection of the database, the server on which it resides, and appropriate network access controls. Teradata highly recommends that customers implement appropriate network perimeter security controls (e.g., firewalls, gateways, etc.) to protect network access to a data warehouse. Additionally, for data warehouse systems deployed on Microsoft® Windows®-based operating systems, Teradata highly recommends that such systems be protected by antivirus software and up-to-date virus definition files.

The remainder of this paper will specifically discuss some of the security features that can be used to effectively secure a Teradata Database.

Teradata Solutions Methodology

Teradata believes that organizations with data warehouses that consolidate and centralize the management of sensitive data are in a much better position to manage security and privacy than those with such data spread across multiple operational or data mart systems. To that end, Teradata has developed an end-to-end capability for designing and implementing secure, privacy-aware data warehouses.

Teradata Solutions Methodology, as depicted in Figure 2, is a formal, proven, patented approach to data warehousing based on integrated processes and customized tools refined through use at the world’s most successful data warehouse implementations. Teradata Solutions Methodology comprises a comprehensive set of privacy and security project features.
For example, the *Analyze* phase includes services to specifically collect and analyze all of the information necessary to integrate data warehouse security into an existing security infrastructure. It considers any current processes by which security and privacy may be implemented for new systems and applications, the information security and privacy infrastructure already in place, and any tools used.

The *Design* phase ensures that the database design and data model fully address all identified privacy and security requirements. Such tasks include identifying data fields that reveal customer identity, identifying data fields containing personal data, identifying data fields containing special categories of data, and adding consent flags for individual privacy preferences that are tied to personal data fields and their uses.

The *Build* phase creates the database administration processes for security and privacy. Implementation includes the definition of Views for making personal data anonymous for analysis purposes. This methodology, implemented by experienced Teradata consultants, ensures that a Teradata Warehouse implementation appropriately considers the impact of all privacy and security requirements.

**Teradata Database Security Features**

Teradata is continuously adding security features to its products. We are committed to driving significant benefit for our customers now and into the future, and to achieving our vision for a leadership role in data warehouse security.

The following sections describe some of the security features that aid Teradata Database clients in effectively implementing a data warehouse security policy, and highlight some attributes and intended usage of these features.

**Authentication**

Authentication refers to the process of establishing the legitimacy of a user before allowing access to database resources. Proper authentication of users is fundamental to ensuring the security of any database system. The Teradata Database provides multiple options for authenticating database users. Additionally, custom authentication methods can be developed and deployed to further enable integration of a Teradata solution into diverse security management environments.

All supported authentication methods are described by a set of properties that can be managed by a security administrator. These properties allow for the security administrator to establish default authentication methods and to restrict or limit the methods that may be selected by a database user. Other properties may similarly be managed by the security administrator.
User-Level Security Controls

Typically, a database user must provide a valid username and password as part of the logon string in order for a database session to be established. However, properly securing such password-based schemes requires that a security administrator be able to ensure that passwords are regularly changed, are sufficiently complex, and that effective precautions can be taken to protect against attempts to guess user passwords. As such, the Teradata Database supports a rich set of password security controls that can be specified at either the user level or the system level. This is important since it is often desirable to establish and enforce different password management policies for different types of database users (e.g., batch versus interactive).

User-level controls are implemented using the User Profiles feature that was introduced in Teradata Warehouse 7.0. In this manner, profiles specifying specific password management policies can be defined and assigned to individual users, groups of users, or an entire enterprise. When a user logs on to the Teradata Database, any associated profile password controls will take effect. If no associated profile password controls have been defined, then the system-level controls will take effect.

Figure 3 describes the password security controls that are supported in Teradata Database V2R6.1 (reference the Security Administration reference manual for implementation specifics)."
to the Teradata Database, database users are not required to provide a username and password as part of the logon protocol. Rather, the system will determine the user’s Windows identity and authenticate the user using the underlying Microsoft Security Service Provider Interface (SSPI). Users may be authenticated using either the Windows NT® LAN Manager (NTLM) or Kerberos protocols as appropriate. Figure 4 depicts the relationship between users, the Teradata Database server, and Microsoft Active Directory in implementing Windows single sign-on.

**LDAP Authentication**

For enterprises where users may have access to many applications and systems, it is common to manage separate user accounts for each application resulting in redundant and/or inconsistent data and increased user management costs. This lack of centralization also represents a significant security risk because unused or expired accounts and privileges are subject to misuse. As such, many enterprises are adopting centralized security management frameworks that provide for a single point of administration for internal and external users, configuration information, and security policies. Such systems can often simplify the process of creating, modifying, and deleting user accounts, as well as authorizing access to protected resources.

These systems typically store and manage user information through a directory service that supports the Lightweight Directory Access Protocol (LDAP). LDAP-enabled applications, services, and databases can readily leverage a single, centralized repository of user information to control user access.

The Teradata Database supports an LDAP authentication method that allows for authentication of database users against a centralized LDAP directory rather than using credentials maintained in the data dictionary. This method authenticates a user (by means of the user’s distinguished name and password) through a secure LDAPv3 bind to the directory. This feature was introduced in Teradata Warehouse 8.0.

**Extensible User Authentication**

Many enterprises have made significant investments in infrastructure technologies, such as user, identity, or access management systems, which provide enhanced support for the authentication and authorization of user access to systems and applications. Many of these systems also support single sign-on architectures wherein session credentials are created upon initial log on to a network or to a supported application. Subsequent logons to other supported applications can use the session credentials for authentication and authorization without requiring additional interaction with the user. While the Teradata Database offers a number
of options for authenticating database users, it is often desirable to integrate the authentication with that provided by such access management systems.

With Teradata Warehouse 8.0, the Teradata Database supports an Extensible User Authentication architecture that allows for custom authentication methods to be developed (with the assistance of Teradata Professional Services) and used for authentication of database users. This architecture is built around the use of standard application programming interfaces, such as the Generic Security Services API (GSS-API) and the Security Service Provider Interface (SSPI). As such, new methods can be developed and deployed without requiring new releases of base Teradata client and database software.

The architecture readily accommodates different types of credentials (e.g., tokens and certificates) that can be used to identify and authenticate a user. Moreover, custom methods can be developed to implement agents that interface to external access or policy servers thereby extending the authentication or single sign-on services provided to include the Teradata Database. Teradata Warehouse 8.1 provides a Software Developer’s Kit (SDK) to support easier development and testing of custom authentication methods. The SDK includes a test framework that enables initial development and testing of new authentication methods without requiring installation on an active system.

**Authorization**

Ensuring appropriate and authorized access to data is a major objective – and concern – in database security. The Teradata Database contains a robust set of fully integrated system access control capabilities. The mission of security administration on a Teradata Database system is to prevent unauthorized persons from accessing the system and its resources, as well as permitting legitimate users access to those resources to which they are authorized. The Teradata Database supports a discretionary access control policy in which access to database objects is restricted based upon the identity of users and/or groups to which they belong. The controls are discretionary in the sense that a user with certain access permissions is capable of passing those permissions on to other users.

**Security Roles**

One of the most challenging problems in managing large data warehouse systems is the complexity of security administration. Often, security administration is costly and prone to errors because security administrators must specify access controls individually for each database user. Role-based access control (RBAC) is a technology that can reduce the complexity and cost of security administration in large data warehouse environments. With RBAC, security is managed at a level that more closely corresponds to an organization’s structure. Each database user may be assigned one or more roles with each role assigning access rights or privileges that are permitted to users in that role. Security administration with RBAC requires determining the operations that must be allowed by users in particular jobs and assigning those users to the proper roles. RBAC effectively manages complexities resulting from differing roles or hierarchies, thereby easing the task of security administration.

Introduced in Teradata Warehouse 7.0, the Teradata Database provides support for Security Roles, which are used to define access privileges on database objects. For example, a user who is a member of a role can access the specific views for which the role has been granted appropriate access rights or privileges. For enterprise data warehouses that provide access to many users, the use of roles will significantly simplify access rights administration and enhance overall security. A security administrator can create different roles for different job functions and responsibilities. For example, a security administrator can grant rights on a clinician view to a role and have these rights automatically applied to all users assigned to that role (Figure 5).

Management of access rights is simplified by allowing grants and revokes of multiple
Security Features in Teradata Database

<table>
<thead>
<tr>
<th>Users</th>
<th>Roles</th>
<th>Views</th>
<th>Base Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinician</td>
<td>Clinician</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinician</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Researcher</td>
<td>Researcher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab Analyst</td>
<td>Lab Analyst</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5. Security Roles**

access rights with one request. This is important when a user changes job functions (role) within the company. Should a job function need a new access right, it can be granted to the role and would be effective immediately for all users with that role.

To effectively use the Security Roles feature, individual rights must be converted into role rights. This requires creating the required roles and granting appropriate rights to each role. Roles can then be granted to users and users assigned their default roles. Finally, all individual access rights that have been replaced by role rights should be revoked from the users to ensure that all access rights are only granted through the role definition.

Typically, only one role will be the session's current or active role. Enabled roles are the current role plus any nested roles. At logon, the current role is the user's default role. Alternatively, it is possible to enable all roles granted to a user for a session.

**Directory Integration**

As noted earlier, many enterprises are adopting centralized security management frameworks, built using LDAP directory services, which provide for a single point of administration for users and associated security policies. Often, with such systems, the directory maintains access control policies that may be enforced by applications to authorize user access to enterprise resources.

With Teradata Warehouse 8.0, Teradata has defined directory schema attributes and objects that allow for the extension of a directory schema to map the distinguished name of a directory user to a Teradata Database permanent user. Such users inherit the roles assigned to the mapped permanent user. However, additional external roles can be created and assigned to the directory user. External roles assigned to a directory user can be used in addition to any roles inherited from the mapped permanent user. A user profile may be created and assigned to a directory user in a similar manner.

These schema extensions are provided for popular directory services such as Microsoft Active Directory and Sun Java System Directory Server. Upon successful authentication, Teradata Database will enable the specified security role(s) and user profile for the database session.

Normally, users are defined in the database via a CREATE USER request. However, some data warehouse environments may support large numbers of users that do not have unique system requirements (such as the need for PERM space or unique SPOOL or TEMP space allocations). To simplify the management of such users, the Directory Integration feature allows for user access without requiring the creation of a database instance for every user. Users that are not
Security Features in Teradata Database

mapped in the directory to an existing permanent Teradata Database user may be mapped to a system-defined user called EXTUSER. Access rights for such external users are determined by the user’s directory-assigned security role(s). Space allocations may default or can be determined by the user’s directory-assigned user profile.

With Teradata Warehouse 8.1, the LDAP authentication method properties can be configured to allow for directory users that correspond to a user defined in the database to log on without requiring directory schema extensions. In this scenario, authorization to access database objects is managed entirely within the database.

Tools are provided to validate directory content and the operation of the directory when using the Teradata schema extensions.

Data Security
It is important to implement appropriate controls to protect sensitive data. Data can be vulnerable when transmitted over non-secure networks or when appropriate access controls have not been enabled for stored data. The Teradata Database provides facilities to manage the encryption of sensitive data when transmitted over non-secure networks. Further, row- and column-level security can be implemented readily using database views.

Network Traffic Encryption
The Teradata Database and associated client applications and utilities typically operate in a traditional client/server environment. If clients are accessing the database server over non-secure networks, there is a risk that data may be compromised by a malicious user who is snooping on the network.

To mitigate this risk, Teradata Warehouse 8.0 provides for encryption of data transmitted between client applications and the Teradata Database. Encryption is a CPU-intensive function that can negatively affect the performance of some operations. As such, its use should be carefully considered. The use of encryption is determined by the user through the client application and can be controlled on a per request basis. As such, the user has complete flexibility in the use of encryption to protect payloads transmitted over a network and to minimize any negative performance impacts. Alternatively, the client interfaces can be configured such that all sessions between the client applications and the database server are encrypted.

The security provided by encryption is dependent upon the strength of the encryption algorithm and the security of the key used to perform the encryption. The Teradata Database uses the public-key based Diffie-Hellman key agreement protocol to generate a secure 128-bit key for use by the client and the database. A unique key is generated for each database session. The key generation is built into the underlying client/server communication protocol thereby eliminating the need for complex key management processes. Strong encryption is accomplished using the industry-standard Advanced Encryption Standard (AES) algorithm.

In networked environments, a password transmitted from a client application to a database server may pose a security risk. If the password is transmitted in clear text over a non-secure network, there is a risk it could be intercepted by a malicious user snooping for data on the network. To protect against this, the Teradata Database client tools and utilities always encrypt the logon string (including username and password) that is transmitted to the Teradata Database server.

For compatibility purposes, the client and server are not required to be at the same version level. However, only the security features common to each version level can be used. This can allow for security features to be utilized according to individual client needs.

Row- and Column-Level Security
Database views are used to restrict the rows and columns that users (or groups of users) can access. Views are part of the SQL standard and can be thought of as virtual tables that can be accessed as if they were physical tables to retrieve data from the database. Views can be defined to reference columns or rows from underlying views and/or tables. A view does not actually contain data but rather is used to provide users with their own logical view of the data within the database. Figure 6
Security Features in Teradata Database

depicts an example from the healthcare industry where researchers, clinicians, lab analysts, and business analysts each represent a specific group of users with their own view of the database. These views enforce different security policies and access rights and privileges by limiting the data elements that are visible by each view.

Teradata Database support for views is particularly high performance because the optimizer generates optimized SQL for selecting the appropriate columns and rows from the underlying base tables. Additionally, query access through views can generate very complex SQL expressions, which further exploit the inherent parallelism of the Teradata Database architecture.

**Auditing and Monitoring**

An important aspect of any security implementation is the creation and monitoring of a record of system activity to detect abnormal activity and to ensure that users are held accountable for their actions. To detect intruders and ensure data integrity, the Teradata Database provides a comprehensive set of auditing capabilities. A security administrator can periodically audit events on the Teradata Database to effectively detect potential attempts to gain unauthorized access to database resources or attempts to alter the behavior of the auditing facilities.

The Teradata Database automatically audits all logon and logoff activity. However, the security administrator can also configure the system’s Access Log to log any successful and/or unsuccessful attempt to access any or all database objects by any or all database users. Also, the Access Log has controls to filter the logging by frequency of access or type of access.

Teradata Database security features include the option to log the SQL expression that was used to perform the access to a database object. As such, all accesses are effectively audited.

Parameterized macros or triggers may be used to further customize or refine the auditing. Triggers are particularly useful when creating audit logs based upon specific data or content-based rules.

All audit information is stored in protected database tables within the data dictionary and access to the information requires appropriate access rights and privileges. The audit records can be viewed through ad hoc queries or with any appropriate application or query tool. Additionally, Teradata Manager includes facilities that enable the security administrator to access preconfigured reports or to generate custom reports from the Access Log.

**Assurance**

Assurance refers to a level of confidence that a product’s security features have been evaluated against a well-defined and widely accepted set of security requirements. Security evaluations are conducted by independent, licensed, and accredited organizations most often to the require-
Security Features in Teradata Database

Security Evaluation under Common Criteria
Teradata Database V2R5.0.2 has been independently evaluated to the requirements of the Common Criteria for Information Technology Security Evaluation (Common Criteria) standard. The Common Criteria is a multi-part standard that aligns with the International Standard ISO/IEC 15408:1999, which is meant to be used as a basis for evaluating security properties of Information Technology (IT) products and systems. The Common Criteria are defined by seven governmental security organizations known as “the Common Criteria Project Sponsoring Organizations” represented by Canada, France, Germany, the Netherlands, United Kingdom, the U.S. National Institute of Standards and Technology, and the U.S. National Security Agency.

The security evaluation of the Teradata Database was conducted by the Booz Allen Common Criteria Test Lab under the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (CCEVS). The Teradata Database was evaluated against 31 separate security functional requirements that describe the security behavior of the system. These requirements span multiple functional classes including Identification and Authentication, User Data Protection, Access, Security Audit, Security Management, and others. While the evaluation considered the design of the system, it also considered processes used for testing and installation and included a vulnerability analysis. As such, this evaluation provides a high level of assurance in the security design and implementation of a Teradata Database system.

This evaluation is intended to satisfy the requirements of those customers (primarily government agencies) that are required to procure only IT systems for which the security robustness has been formally evaluated and validated.

Teradata Database Security Advantage
Teradata has a defined architecture for protecting personal information or other confidential data within a database. Important patents protect this intellectual property:

- U.S. Patent # 6,253,203 – Privacy-enabled database (issued June 26, 2001)
- U.S. Patent # 6,275,824 – System and method for managing data privacy in a database management system (issued August 14, 2001)
- U.S. Patent # 6,438,544 – Method and apparatus for dynamic discovery of data model allowing customization of consumer applications accessing privacy data (issued August 20, 2002)
- U.S. Patent # 6,480,850 – System and method for managing data privacy in a database management system including a dependently connected privacy data mart (issued November 12, 2002)

The architecture represented by these patents leverages core Teradata Database strengths such as:

- The ability to store and manage large volumes of detailed data through support for normalized data models, an infrastructure that efficiently enables multiple views, and data models that are easily extended.
- A high-performance implementation that makes views practical for privacy. Optimized SQL selects appropriate columns and rows from base tables, and complex SQL expressions exploit Teradata Database parallelism.
- A security mechanism that can deny access to restricted views or macros.
Security Features in Teradata Database

> Access logging that provides a privacy audit trail and includes options to log all accesses (or access attempts) to a table (or view, macro), and log the associated SQL expression.

**Conclusion**

The Teradata Database provides a rich set of security controls for managing, protecting, and auditing access to stored data. These capabilities include extensive password controls, support for multiple authentication methods, access controls, high-performance database views, network traffic encryption, access logging, and audit reporting.

New industry regulations, especially in the retail, financial services, and healthcare industries, present increased challenges for securing an enterprise’s information assets. The security capabilities described in this paper can assist Teradata Database security administrators in meeting these new challenges.

**Endnotes**

