Security Features in the Teradata Database

Jim Browning

02.15 EB1895 SECURITY

TERADATA.

Table of Contents

Abstract

The Teradata® Database supports many important features that are designed to enhance the security of an integrated 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.

Security Challenges

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'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. The 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 maintenance and transmission of 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 of 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 containing consumer or employee information on more than 5000 persons. 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 twelve 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[1] 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."

1 Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model

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.

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

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 achieve 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 data warehouse 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 selectable 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).

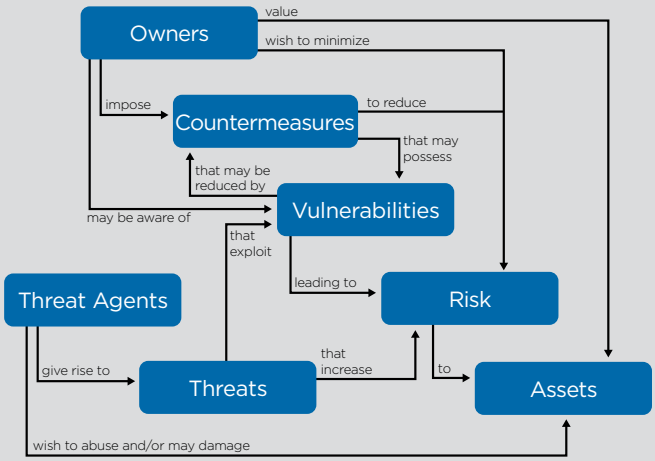

Figure 1. Security Concepts and Relationships.

User-level controls are implemented using the User Profiles feature. 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 2. describes the password security controls that are supported by the Teradata Database (reference the *Security Administration* reference manual for implementation specifics[2]).

2 Teradata Database Security Administration – www.info.teradata.com

Usage Controls	Description
Password Expiration	Allows the security administrator to define a time span during which a password is valid. After the time elapses, the user must change the password.
Password Reuse	Allows the security administrator to define the time span that must elapse before a previously used password can be reassigned to a user.
Maximum Logon Attempts	Allows the security administrator to define the number of erroneous sequential logon attempts a user is allowed before the user is locked to further logon attempts.
Password Lockout time	Allows the security administrator to sets the user lock time duration after the user has exceeded the maximum number of logon attempts.
Format Controls	**Description**
Password Length	Allows the security administrator to define the minimum and maximum number of characters required in a valid password string.
Password Construction	Allows the security administrator to specify whether alpha characters, digits, special characters, and a combination of upper and lower case characters are to be allowed or required in the password string. Also, allows the security administrator to specify whether the username or dictionary words should be allowed to be included in the password string.

Figure 2. Password Controls

Single Sign-on

Effective user authentication is a foundation of a database system's security services. However, secure authentication may be compromised in large, heterogeneous networks where users may be required to remember multiple user names and passwords. To address this issue, a single sign-on capability can be employed to allow network users to seamlessly access authorized network resources and applications, including an integrated data warehouse, with a single authentication that is performed upon initial network access. This capability improves the productivity of network users, reduces the cost of network operations, and, ultimately, improves network security. Further, security is improved by eliminating the need for an application to declare or store a password on the client system.

The Teradata Database supports single sign-on (SSO) of users that have successfully authenticated to a Windows domain or Linux Kerberos realm. With SSO, a user does not provide any credentials (user ID or password) when initiating a logon to the database. Rather, the user will be identified and authenticated based upon his/her current domain-authenticated session. Kerberos V5 is the protocol used to facilitate SSO of users to the Teradata Database. Figure 3 depicts the relationship between users, the Teradata Database server, and Microsoft Active Directory in implementing 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 in that 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.

Trusted Sessions

The Teradata Database support a Trusted Sessions feature that can be used to preserve the security model commonly used by middle-tier and web-based application systems. This features provides the ability to authorize a limited trust model that allows middle-tier applications to assert user identities and roles through pooled connections. Eliminating the need to authenticate (or re-authenticate) users accessing the database through a middle-tier results in improved performance, scalability, and support for large numbers of users. It also enables greater granularity of access rights enforcement and auditing of access based upon end-user identity.

IP Filters

IP Filters can be defined to restrict the use of non-interactive logons (used for batch load jobs, middle-tier application connection pools, web services, etc.) by client system IP address or network subnet. Restricting the use of these user logons to specific client or server machines helps mitigate the associated security risk since a hacker would also have to compromise a specific machine in order to effectively logon to the database.

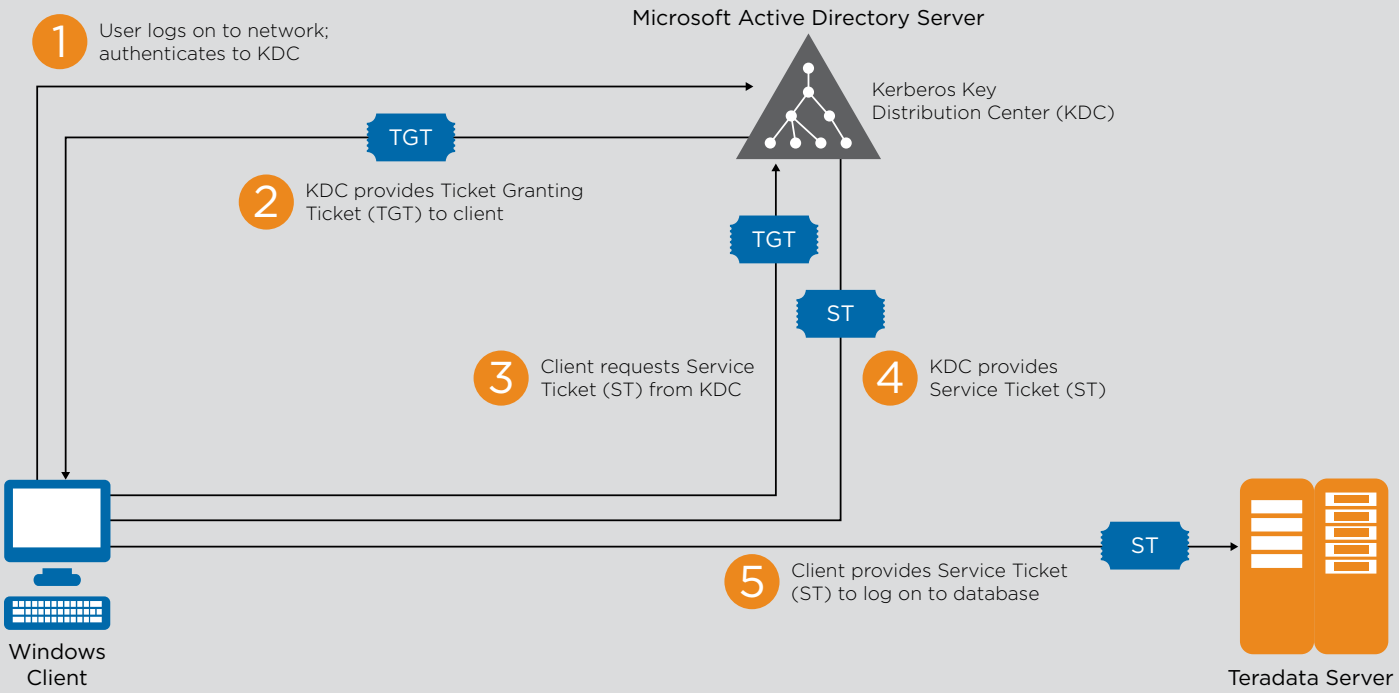

Figure 3. Kerberos-based Single Sign-on.

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 that 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.

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 integrated 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 4.).

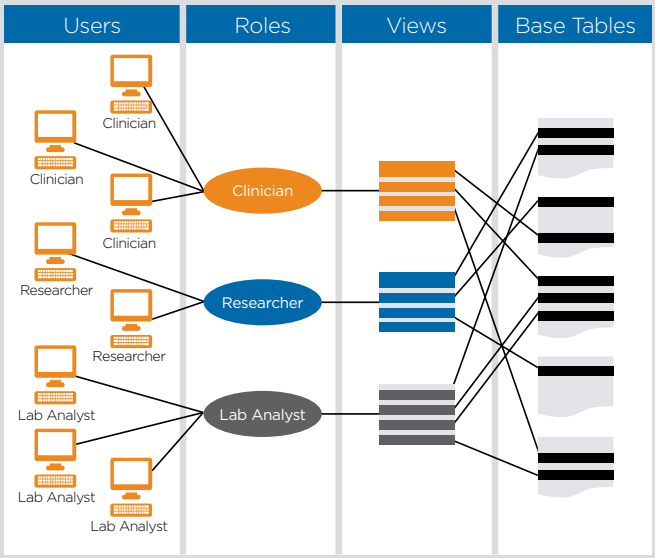

Figure 4. Security Roles.

Management of access rights is simplified by allowing grants and revokes of multiple 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.

Teradata has defined directory object mappings that allow for the mapping of 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. Upon successful authentication, the Teradata Database will enable the specified security role(s) and user profile for the database session.

The LDAP authentication method properties can be configured to allow for directory users that correspond to a user defined in the database to logon without requiring directory mappings. 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 readily be implemented 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, the Teradata Database and client tools support 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 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 with support for 128-bit, 192-bit, or 256-bit keys.

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.

Full Disk Encryption

Some Teradata Appliances and Active Enterprise Data Warehouse systems support an optional full disk encryption capability implemented using self-encrypting drive (SED) devices within the storage arrays. Access to the data stored in an SED device requires an authentication key which is stored externally to the SED device and used by the storage initiator to "unlock" the device and enable READ/WRITE operations. Until a successful authentication has occurred the SED device will not respond to READ/WRITE requests. Once authentication has succeeded then the encryption key stored internally to the SED device is accessed and used by the device for encryption and decryption of the data stored and retrieved from the devices. Encryption is performed using AES-256.

Data Encryption

To protect sensitive data from internal and external threats, the Protegrity Database Protector for Teradata provides support for selective, and highly secure, column-level data encryption. A security administrator can centrally define, distribute, and enforce encryption policies independently from database administration with a full range of secure audit reports that provide complete accountability of access to secure data.

Data is encrypted using any of several supported industry-standard cryptographic algorithms in combination with initialization vectors to prevent statistical attacks and checksums on encrypted data to detect malicious attempts to manipulate the data. This capability provides centralization of all key management tasks on a single platform and effectively automates key management and administration, including an automated and secure mechanism for key rotation, replication, and backup.

The Protegrity Database Protector also supports tokenization which can often be used as an alternative to encryption for protection of sensitive data. This approach is governed by the same security policy and access control rules as used for encryption. Where tokens can be used in place of original data, this approach can eliminate much of the performance overhead commonly associated with the use of encryption.

The design fully exploits the parallelism provided by the Teradata Database to maximize database performance when querying encrypted data.

Teradata BAR Encryption

As part of Teradata's Backup, Archive, and Restore (BAR) architecture, encryption of backups and archives is supported through hardware-based encryption for LTO5 and LTO6 tape drives on Quantum i500 and i6000 libraries. Encryption is managed by two Scalar Key Management Appliances and is supported for backup-to-tape or copy-from-disk/tape. Encryption is performed using AES with 256-bit keys and does not affect the performance of backup or restore operations.

Encryption of backups to disk is supported using the EMC Data Domain DD4200 Deduplication Storage System. This system provides inline data encryption with compression. The encryption is performed using AES with 128-bit or 256-bit keys and implemented using FIPS 140-2 validated RSA BSafe cryptographic libraries.

Row and Column-level Security

The Teradata Database supports the granting and revoking of SELECT, INSERT, and UPDATE rights at the column level.

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

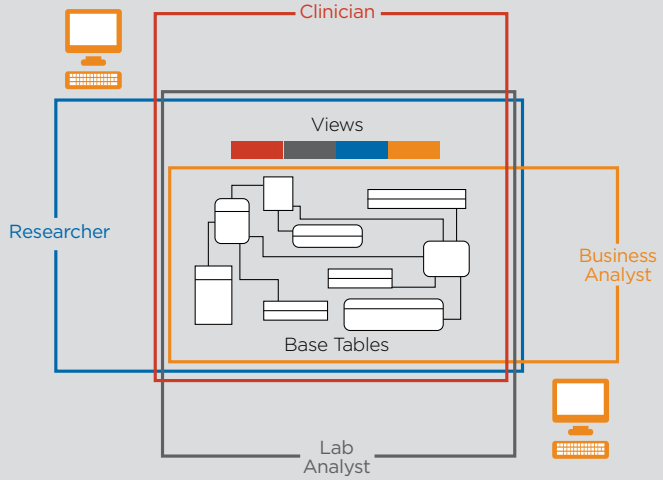

Figure 5. Database Views.

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 5 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 in that 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.

The Teradata Row Level Security option can be used to restrict the rows of data that users (or groups of users) can access. It uses customer written policy functions to filter access based on the data in the row and the user submitting the query. Restrictions based on data sensitivity or ownership and access authorization can be easily enforced using Teradata Row Level Security.

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 additionally 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.

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 requirements of a specific industry standard. A security evaluation provides assurance through an analysis of a system's security functions using functional and interface specifications, guidance documentation, and the high-level design of the system to understand the security behavior. Independent testing of the security functions supports the analysis, evidence of developer testing based on a functional specification, selective independent confirmation of the developer test results, and a search for obvious vulnerabilities. Assurance is also provided through a configuration list for the system and evidence of secure delivery procedures.

Security Evaluation under Common Criteria

The Teradata Database 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 15408:2005, 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 evaluation, conducted by the Science Applications International Corporation (SAIC) Common Criteria Test Lab under the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (CCEVS), determined that the evaluation assurance level (EAL) for the product is EAL 4 augmented with ALC_FLR.3. The Teradata Database has been evaluated against 25 separate security functional requirements that describe the security behavior of the system. These requirements spanned 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.

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 support many existing features within the Teradata Integrated Data Warehouse (IDW) and can assist Teradata Database security administrators in meeting these new challenges.

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com**

02.15 EB1895

TERADATA.