C2 SECURE DATABASE MANAGEMENT SYSTEMS – A COMPARATIVE STUDY

Ramzi A. Haraty
Lebanese American University
P.O. Box 13-5053
Beirut, Lebanon
rharaty@lau.edu.lb

KEYWORDS

Audit, Discretionary Access Control, and Security Policy.

ABSTRACT

In this paper we discuss the architecture, security policy, and protection mechanisms of four National Security Agency – C2 certified database management systems. We compare their techniques used for protecting the database against users who are not authorized to access a part of the database or the whole database.

1. INTRODUCTION

As the number of database users and the size and value of databases increase, the security of the databases becomes of paramount importance. Although many database management systems (DBMSs) provide some form of data security, they are not evaluated or certified by the National Security Agency's (NSA) Trusted Product Evaluation Program. Therefore, little trust can be placed into these unevaluated systems to adequately protect confidential and proprietary information. This paper only concentrates on the NSA evaluated DBMSs that achieved at least the C2 level of trust. Systems at the C2 level enforce a finely grained discretionary access control making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation [1][2]. These evaluated DBMSs are:

- International Business Machines' AS/400 Version 2 Release 3, which was made available to customers in July of 1996,
- Informix Corporation's Informix OnLine/Secure Version 4 Release 1, which was released in 1991,
- Oracle Corporation's Oracle 7, which completed evaluation in April 1994, and
- Sybase Corporation's SQL Server Version 11.0.6., which was released in December 1996.

Any discussion of security begins with a description of the security policy, i.e., the set of rules that are used to determine whether a given user can be permitted to gain access to a given data item. There are generally two types of security policies [3]:

- Discretionary Access Control (DAC) is used to control access between users and data based on a need-to-know, and
- Mandatory Access Control (MAC) is used to enforce multilevel security whereby users and data are classified into various security classes.

Although some of the above DBMSs provide MAC-level protection, this paper only concentrates on DAC and discusses the architecture, security policy, and protection mechanisms (namely, identification and authentication, audit, and object reuse) of each evaluated DBMS. This paper is organized is follows: Section 2 presents the architecture of these DBMSs. Section 3 discusses their security policy. In section 4, the identification and authentication mechanism is discussed. Section 5 presents their audit features. Section 6 presents their object reuse policy, and finally, section 7 contains the conclusion.

2. ARCHITECTURE

IBM

The AS/400 DBMS implements the relational data model and is fully integrated with the OS/400 operating system [5]. Its functionality is supported by the operating system. There is no single definable piece called a DBMS. Instead, there are components at the various layers of the operating system that provide DBMS functions. For example, at the OS/400 layer, there are direct commands to create, destroy, and display database files, as well as a query interface and an Structured Query Language (SQL) interface, among others. At the Vertical Licensed Internal Code (VLIC) layer, there are components that support these

SAC '99, San Antonio, Texas

interfaces and database functions such as audit management. In addition, the database functionality relies on the VLIC components to provide I/O and other services that are used by all components.

The AS/400 provides end users with several interfaces to define and access data stored in database files. These interfaces vary from command-based interface to graphical user interface using forms and menus.

INFORMIX

Informix-OnLine/Secure runs as a trusted process on either AT&T's System V/MLS, Harris Computer Systems' CX/SX, Harris Computer Systems' CX/SX with LAN/SX, or Hewlett Packard's HP-UX BLS operating system.

Informix-OnLine/Secure supports three different security configurations [4]. The first is the Enhanced Assurance; it provides the highest degree of assurance by isolating the security relevant portion of the product. An Enhanced Performance (EP) configuration may also be installed, which adds the SQL engine to the security portion of the product for performance enhancements. Lastly, there is the C2 configuration. The C2 configuration is a subset of the EP configuration.

Each configuration contains the same architectural components. These components are: the secure administrator front end, the administrator front end, the user front end, the SQL engine, relational storage access methods, support processes, daemon processes, transient processes, and global shared memory.

ORACLE

Oracle executes as an application within the context of the operating system. Oracle runs on the HP-UX BLS operating system. Oracle provides concurrent multi-user access to the information stored within a relational database [6]. In addition to access control, Oracle provides features for query processing, stored procedure execution, transaction management, and database recovery.

Each user actively accessing a database is associated with both a user process and an Oracle server process. The user process is simply a process that can invoke Oracle functions as well as operating system functions. The Oracle server process accesses database files on behalf of the user process. The server process accepts requests for the database operations from the user process, performs the operations, and communicates the results back to the user process.

In addition to the server process associated with each user, there is a set of background processes for each database. All of the server and background processes execute the same executable file. Consequently, all of these Oracle processes have access to the files containing the database and to an associated area of shared memory that contains buffers and the information needed to coordinate the activities of the Oracle server and background processes.

SYBASE

The Sybase SQL Server (hereafter referred to as the server) executes as an application within the context of the operating system [7]. It runs on the NSA-certified HP-UX BLS operating system. It is based on the client-server architecture. Each user is associated with a client process that communicates with a server task via a communication interface using Sybase's Tabular Data Stream protocol. The server is multithreaded; it can handle multiple concurrent client requests. The client process executes on one machine and communicates with a server on the same machine.

The server runs as multiple processes on the underlying operating system. Each server runs as one or more separate processes, each process being referred to as an engine. Communication between engines is achieved primarily through shared memory segments, a resource provided and protected by the operating system.

3. SECURITY POLICY

IBM

The AS/400 allows users to protect objects using authorities (permissions) and authorization lists. In addition, the system also requires users to have special authorities to access certain objects by commands and application programming interface and other special privilege instructions.

Authorities can be granted to users, groups of users, and all users. There are three types of authorities: owner, private, and public. Owner authority refers to the authority of the owning user profile (which represents a user). All objects on the system have an associated owner. Private authority refers to an authority that is explicitly granted to a particular user profile. Private authorities to objects are stored in the user and/or group user profile. Public authority applies to all users on the system. The public authority is used in the absence of owner or private authority.

The AS/400 system checks access to objects at the OS/400 level and at the VLIC level. Although there are several ways to invoke an access check, the algorithm that is used to verify authority is the same.

INFORMIX

The Informix-OnLine/Secure DAC mechanism has the ability to include or exclude access to DBMS objects on a per user basis, and enables individuals to control

other users' access to these objects. No user can access the information in a database unless that user has been authorized explicitly or by default to access it in accordance with the DAC policy. The Informix-OnLine/Secure DAC mechanism is completely separate from that of the operating system, yet it extends the operating system DAC policy by applying access attributes specific to database objects.

The DAC policy protects information stored in databases up to the granularity of individual columns within given tables. DAC is accomplished via privileges which users grant and revoke using SQL statements. Privileges are granted to single users by name or to all users under the name of *public*. There is no way to create groups or assign privileges to groups.

Tables, views, synonyms, constraints, and indexes all have an owner that is the user who created the object. A database, on the other hand, has a creator that is awarded the *dba* privilege instead of ownership. A privilege is conceptually different from ownership. In order to facilitate transfer of administrative responsibility, the *dba* privilege for a database can be granted to and revoked from another user. The owner of a named object, on the other hand, remains fixed during its lifetime. In addition, one or more users can have the *dba* privilege for a given database, while only a single user can be the owner of a particular named object. A user that possesses the *dba* privilege is also called a database administrator for that database.

ORACLE

The DAC security policy enforced by Oracle is based on the SQL standard, with several additional features. The primary addition is the support of roles to help organize the authorization of privileges into application-specific groups.

Oracle also supports two types of privileges: object privileges and systems privileges. Object privileges are the object access modes for objects and are used for DAC enforcement. System privileges relate to a whole database and provide a broad range of authorizations. System privileges include privileges needed by system administrators and privileges that can be used to bypass the DAC enforcement. Both object and system privileges can be granted to individual users. In addition, roles can be defined and privileges can be granted to individual roles. In effect, a role is a collection of privileges that can, in turn, be granted to users.

SYBASE

The server's DAC policy augments the operating system's DAC policy to apply to DBMS objects. The server associates an Access Control List (ACL) with each object and performs DAC mediation based on those ACL entries. DAC decisions are based on user attributes such as user identity as well as object ownership. The DAC mechanism includes the grant and revoke statements and the DAC algorithm. Grant and revoke are used to give or revoke from users, object creation and object access permissions. The DAC algorithm is executed one grantor at a time. If the user is granted access by the grantor, the algorithm exits and the user is granted access. If the user is denied access for one grantor, the algorithm is executed again for the next grantor. If a user is not granted access by any grantor, then the user does not get access.

4. IDENTIFICTION and AUTHENTICATION

IBM

The AS/400 requires all users to identify and authenticate themselves before they are allowed to access system resources. Users are identified by a user profile and authenticated by a password. Each user has a unique user profile. A password of one to ten characters is used to authenticate users. The password is initially set by the security administrator when the user profile was created. The password can be set to **NONE* that prevents the use of the user profile for interactive sign on.

Data Encryption Standard encryption is used to encrypt the user profile name using the password as a key. The result of this encryption is then compared to the encrypted password stored in the system. If the two values are the same, then the user is authenticated. If the values are different, then the user is allowed to retry the password. The exact number of retries is determined by the security administrator. The AS/400 also can restrict where users are allowed to sign on (physically) by restricting authority to the display stations.

A user may fail to sign on the system due to several reasons. The number of times a user can attempt to sign on the system, and the appropriate actions that the system can take can be set by the security administrator. There are a number of actions that can be taken when the limit is reached: 1) disable display station, 2) disable profile, and 3) disable display station and profile.

INFORMIX

Informix-OnLine/Secure relies solely on the underlying operating system to provide identification and authentication services; therefore, identification and authentication information for the database and the operating system is kept in a central repository protected by the operating system. To ensure that users may not invoke or access information outside their access group, Informix-OnLine/Secure relies on the operating system to properly restrict users from logging into levels or groups to which they do not have access.

ORACLE

Users are identified to Oracle by unique names and Oracle relies on the operating system to provide authentication. Each user must be defined to Oracle as a prerequisite to connecting to Oracle. This requires specification of the username with the *CREATE USER* command. The username is stored in a data dictionary table. Also stored is the Oracle user identification number and the time and date of username creation. The username is used by Oracle to identify the external user associated with a session.

SYBASE

The server supports its own identification and authentication mechanism in addition to that of the underlying operating system. The server maintains user login account information in its own database.

To establish a session with the server, the user must have already established a client process with the underlying operating system, generally by logging in to the operating system. The user must then log into the server to initiate a DBMS session. As a result of a successful login, the user gets represented by a unique identifier which will be used in access mediation.

The server enforces a minimum password length of six bytes and a maximum of 30 bytes, which may include any combination of printable characters. The server rejects any attempt to enter a new password of less than six bytes. The password space varies according to how the supported character set maps into bytes. A standard QWERTY keyboard supports a minimum of 94 printable characters, including upper and lower case, numerals, and special characters, each of which maps to a byte giving a minimum password space size of approximately $94^6 \sim 7 * 10^{11}$ possibilities.

5. AUDIT

IBM

The AS/400 system has the ability to audit all security relevant events. All audit entries are maintained in journal receivers in the security audit journal. The security audit journal serves as a repository of journal receivers that contain the actual audit data. Only authorized users may gain access to the security audit journal and journal receivers. Furthermore, there are no external interfaces available to modify journal entries or to remove individual entries from the journal. Once the entries have been written to the journal, they cannot be modified. Both preselection and postselection options are used to select and analyze audit data.

Auditing of security relevant events in the AS/400 is accomplished by having the software that produces such an action call the appropriate audit routines. If auditing is active and the security action is preselected, then these routines will send appropriate audit entries to the journal receiver in the security audit journal.

When audit data are received from the auditing routines, they are collected in an audit buffer in main storage. The number of audit data entries that can be collected into the audit buffer before being forced to auxiliary storage is defined by the audit administrator, and determine the potential amount of audit loss in the event of unexpected system failure. Whenever certain predefined thresholds are met, the buffer is written to auxiliary storage.

When auditing is turned on for many different actions or many different objects on the system, the AS/400 knows when more than one process is waiting to deposit a journal entry into the audit buffer at the same time. The AS/400 continues to deposit entries into the journal receiver until there are no more processes waiting to deposit an entry or until the audit force level threshold is reached. The AS/400 then does an audit force on the audit buffer for the audit entries deposited in the audit buffer. This audit force will cause the audit buffer to be written from main storage to auxiliary storage.

The audit mechanism also monitors the size of the journal receiver in auxiliary storage. If the journal receiver reaches an audit administrator-specified threshold, the audit mechanism generates warning messages that are sent to the audit administrator. This allows the audit administrator to react to possible journal receiver-full conditions and to keep the system from shutting down.

INFORMIX

Informix OnLine/Secure has the ability to audit all security relevant events. The system security officer chooses the events to be audited and maintains the audit masks. The audit masks indicate which events should cause an audit record to be created and inserted in the operating system's audit log. The audit analysis officer can then extract all the Informix-OnLine/Secure audit logs from the operating system's audit log and performs audit analysis.

An audit mask specifies a set of user events to be audited. The domain of auditable events is fixed; however, the database system security officer is responsible for choosing which events to audit. Audit masks are implemented as a sequence of bits, one for each auditable event. Each individual user always has two masks applied to their actions when using Informix-OnLine/Secure. One is the compulsory mask, the other is either the default mask or an individual user mask.

ORACLE

The Oracle audit facility enables appropriately

privileged users to monitor database activities involving a particular object, a particular type of object, a particular type of operation, or an individual user. The recording of audit information can be enabled or disabled. In addition, the audit trail can be directed to a database table or to the operating system audit trail.

When a command is received, Oracle parses it, and then calls the appropriate audit routine to record audit information. The audit record structure is allocated at the beginning of the parse and populated before the audit record is written out. The action of when to write an audit record depends on whether the parse is successful or not. The audit routine checks the appropriate data dictionary table of that type of object for object auditing options, then an audit data dictionary table for statement options. The check determines whether the action is auditable by access or by session, and to control when the audit record is written. Information for populating the audit record is also determined.

SYBASE

The server provides an audit trail of activities within the server. The audit trail is stored as tables and is separate and independent of the audit trail provided by the operating system. It contains the following information: access to database objects using SQL statements, identification and authentication activities, and other security relevant events (e.g., use of security-relevant system stored procedures).

Audit of SQL statements is done on the basis of access instances to objects, rather than on a per SQL statement basis. This means that a single SQL statement may generate multiple records, each representing access to a single object. Additionally, if a SQL statement accesses multiple objects and an access check fails for one, audit records for the other objects are still generated.

6. OBJECT REUSE

IBM

Object reuse concerns the allocation of resources that have been used to store information and then released back to the system. A user must not be able to scavenge data from resources previously allocated to other users. The AS/400's object reuse policy is twofold: clear storage before reuse, and restrict access to an object until the resource has been written into.

INFORMIX

Informix-OnLine/Secure does not provide any interfaces to an object's resources until the object has been used. An object cannot be read by a user until it has been written into. Resources allocated for an object's use cannot be accessed.

ORACLE

Oracle data structures are either cleared when allocated or initialized with valid data prior to access.

SYBASE

Sybase provides object reuse for internal data structures that contain data visible to a user. These structures are either cleared when allocated or overwritten with the contents of new objects.

7. CONLUSION

Secure DBMSs are fast becoming a reality. In this paper, we presented the four NSA-evaluated secure DBMSs and discussed their architecture, security policy, and their different protection mechanisms. Although they have different architectures and security designs, they all provide assurance commensurate with the C2 level of trust.

REFERNCES

[1] *Department of Defense Trusted Computer System Evaluation Criteria.* DOD 5200.28-STD. December 1985.

[2] *Department of Defense Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria.* DOD 5200.28-STD. April 1991.

[3] ElMasri, R, and Navathe, S. *Fundamentals of Database Systems.* Second Edition. The Benjamin/Cummings Publishing Company, Incorporated. Redwood City, California. 1994.

[4] Final Evaluation Report, *Informix Software, Incorporated INFORMIX-OnLine/Secure.* National Computer Security Center NCSC-FER-94/032. March 21, 1994.

[5] Final Evaluation Report, *International Business Machines Corporation Application System/400.* National Computer Security Center NCSC-FER-95/006.B. October 3, 1997.

[6] Final Evaluation Report, *Oracle Corporation Oracle 7 and Trusted Oracle 7.* National Computer Security Center NCSC-FER-95/006. April 5, 1994.

[7] Final Evaluation Report, *Sybase, Incorporated SQL Server Version 11.0.6 and Secure SQL Server Version 11.0.6.* National Computer Security Center NCSC-FER-96/002. March 3, 1997.