Nuts and Bolts of Database Security

Pradeep Navalkar

M-co, The Marketplace Company Limited (www.m-co.com)

A lot of effort goes into winning a reputation, but yet it is the first thing you could lose. There are several building blocks that go into ensuring that your Oracle database is safe and secure. This paper is aimed at managers and database owners, and describes the essential requirements of database security. This paper is not intended to cover all aspects of database security – it merely offers some guidelines that can be adapted to your organization's security needs.

The paper is divided into two sections. The first part of the paper gives some guidelines for information system security. The second part describes the Oracle Security features.

Providing and ensuring information security sounds both disarmingly easy and bewilderingly difficult. It is both legitimately challenging and totally unfair. It is incredibly rewarding and pull-out-your-hair-and-scream-to-the-heavens aggravating. To some it is a mystery wrapped in riddle inside an enigma.

We hear about various malicious attempts to access organization's confidential information, both from external sources and from within the organization. Setting up a firewall is just not enough, as the security perimeter of an organization seems to have disappeared. We hear about credit card numbers being compromised or stolen by the outside world. Since the inception of credit cards, consumers have been reluctant or worried about giving their credit card numbers over the telephone, or while purchasing goods and services online. For that matter, any personal information requested raises eyebrows. We suddenly realize that confidentiality of information plays an important part in our everyday life.

Organizations that maintain critical information have an increased responsibility to securely store the information and also securely transfer it at all times. The Information System Security Plan of an organization should ensure that Confidentiality, Availability and Integrity of information and the various ICT (Information and Communications Technology) components are maintained at all times. One size does not fit all in many cases and is especially true with a Security Plan. For example, a military-based organization will need confidentiality to be ensured foremost, whereas a banking or commercial organization will need integrity ensured first, and a real-time data provisioning organization will need to ensure availability as its first priority. Hence, each organization will need to come up with its own security plan for their business requirements. Those responsible for the Oracle database security and information stored within the database need to be aware of the organization's Security Plan and also be accountable for it. The database security plan should be derived from the organization's Information System Security Plan.

Information System Security Guidelines

Here are a few guidelines to help ensure that you have a well-defined Information System Security Plan in place.

1. Information System Security Policy
Every organization should have an overall Information System Security Policy that is specific to the organization. The Security Policy will dictate the role security plays within the organization and will outline the goals that the organization needs to meet. It assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out. The policy must address relative laws, regulations, and liability issues and how they are to be satisfied. It should describe the amount of risk management is willing to accept.

Depending on the organization's business needs and size, issue-specific or system-specific Security Policies should be developed. Some examples are an email policy, a password management policy, a database protection policy, and a wireless access policy.

The Security Policy provides a broad overview and covers many subjects in a general fashion. The procedures, standards and guidelines provide the granularity needed to actually support the policy. While the Security Policy provides the foundation, the procedures, standards and guidelines provide the security framework. The Security Policy should be regularly reviewed and updated to keep it current.

2. System Development Practices
Security should be an inherent aspect of any system starting from the project initiation stage. It is very expensive and almost impossible to include security at a later stage. Different environments like client server, e-commerce and web services demand different security needs. Hence, implementing and enforcing standards for software development, Oracle development and database installations will ensure consistency and best practices are followed. User and operator errors are the biggest causes of system malfunctions. For example, checking program input lengths so buffer overflows cannot take place should be a part of the software development standard.

A security plan should be drawn up at the beginning of a development project and integrated into the functional design to ensure that security is not overlooked. Just like project management is an important part of product development, security management should be an important part of project management. Any new technology or product should be assessed against standards.

3. System Change Control
This is a process to ensure that any type of change within the environment is managed, and no original functionality was affected in an adverse way. It includes authorization, documentation and testing of every change.

Configuration management is the process of controlling the life cycle of an application and documenting the necessary change control activities. It outlines the procedures that are used to carry out changes that affect the ICT components.

Change control should be evaluated during system audits. Security testing should include penetration tests and vulnerability tests. The product and software vulnerabilities and threats, risks, exposures, and the de-support notices from vendors should be considered seriously.

Timely patches should be applied to systems and these should also be subject to change control. A term being spoken in recent days is the "zero day" attack, which occurs when a researcher discovers a vulnerability and discloses the flaw to the public without first notifying the vendor. This puts businesses and individuals at risk from the time of the disclosure until the affected vendor issues a patch. Some patches can be made in hours, but even then it takes time for affected machines to download the patches.

4. System Access Control

Access control deals with identification, authentication, authorization and accountability. Organizations should employ Least-privilege and Need-to-know principles. These are based on the concept that individuals should only be given access to the information that they require to perform their job duties successfully. It is important to understand that it is the management's responsibility to determine the security requirements of individuals and how access is authorized.

Organizations may wish to deploy two-factor authentication as a standard. This means the authentication is made up of at least two of the following three aspects: something you know (like PIN or password); something you have (like swipe card or smart card); and something you physical about you (like fingerprint or retina scan).

The ICT components should be securely configured. The default access should always be configured and set up with "no access". At a minimum, logging of successful and unsuccessful attempts should be carried out.

5. Securing the Information

Data and Information needs to be securely stored as well as securely transferred. An organization may wish to hide critical data using an encryption standard, or they may stipulate that confidential information be transferred via email using PGP. SSL uses public key encryption to protect a communication channel, and provides data encryption, server authentication and message integrity.

Two database security issues are aggregation and inference. Aggregation is defined as the act of combining information from separate sources. The combination of two or more pieces of information forms new information; to which the subject does not necessarily have the rights to access. The combined information may have a sensitivity that is greater than the individual parts. Inference is defined as the ability to derive information that is not explicitly available. Content- and Context-dependent access control helps to address these database security

issues. For example, common attempts to prevent inference attacks are cell suppression, partitioning the database, and noise and perturbation.

6. Physical and Operations Security

Physical security mechanisms include site design and layout, environmental components like HVAC (Heat, Ventilation and Air-Conditioning), emergency response readiness, intrusion detection, and power and fire protection. These mechanisms protect people, data, equipment, systems, and the facility itself. Access to key physical areas like server rooms should be provided only after appropriate authentication and authorization.

Operations security involves the continual maintenance of an environment, and the routine activities that enable the information systems to run correctly and securely. This includes areas of security operations like media controls, system controls, and input and output controls. Data remanence is the residual physical representation of information that was saved and then erased in some fashion. This remanence may be enough to enable the data to be reconstructed and restored back into a readable form. This can cause a security threat to an organization that thought their confidential data was properly erased from their media. If the data is sensitive, degaussing, or physical destruction of the media may be required.

7. Disaster Recovery Plan

Disaster recovery has the goal of minimizing the effects of a disaster and taking the necessary steps to ensure that the system resources, personnel and business processes are able to resume operation in a timely manner. The disaster recovery plan will be carried out when everything is still in emergency mode and the team is scrambling to get critical systems back online.

Several mechanisms can be put in place to ensure that an organization can recover from outages and disasters. Regular backups of critical data should be carried out. The backups are useless if they cannot be restored, hence periodically the backups should be restored in test environments. The organization must decide whether it needs an offsite backup facility, like a hot site, warm site or a cold site. Human resources are a critical component to any recovery process, and their requirements need to be fully thought out and integrated into the plan. Tests and disaster recovery drills should be performed at least once a year. These will demonstrate to management whether an organization can actually recover after a disaster.

Most organizations cannot afford for the disaster recovery tests to interrupt production; hence the appropriate type of drill should be chosen. The types of drills are Checklist Test, Structured Walk-through Test, Simulation Test, Parallel Test and Full-Interruption Test. In a Structured Walk-Through Test, the group will walk through different scenarios of the plan from beginning to end to make sure nothing was left out. This also raises the awareness of the recovery procedures to team members.

8. Business Continuity Plan

Organizations that survive disasters are those that thought ahead, planned for the worst, estimated the possible damages that could occur and put the necessary controls in place to protect themselves. Business Continuity Planning (BCP) provides methods and procedures for

dealing with longer-term outages and disasters. Business Continuity Planning takes a longer look at the problem. This includes getting critical systems to another environment while repair of the original facility is taking place, getting the right people to the right places, and performing business in a different mode until regular conditions are back in place. It also involves dealing with customers, partners and shareholders through different channels until everything returns to normal.
Management must be convinced of the necessity for a business continuity plan.

Business Impact Analysis helps an organization to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the organization's critical systems needed for survival and estimates the outage time that can be tolerated by the organization.

Risk Analysis is a method of identifying risks and assessing the possible damage in order to justify security safeguards. Risk analysis provides a cost/benefit comparison where the annualized cost of safeguards to protect against threats is compared with the expected cost of loss. Some formulae used in the quantitative risk analysis are:
Asset Value x Exposure Factor (EF) = Single Loss Expectancy (SLE)
SLE x Annual Rate of Occurrence (ARO) = Annualized Loss Expectancy (ALE)
where *EF = percentage of asset loss caused by identified threat*
ARO = Estimated frequency a threat will occur within a year

9. Staff and User Training and Awareness
Security awareness training needs to be provided to staff and system users on a regular basis. People are usually the weakest link, and cause the most security breaches and compromises. If employees and users understand how to properly access resources, why access controls are in place, and the ramifications for not using these access controls properly, an organization can reduce many of the types of security incidents that take place.

10. Management Ownership and Support
The management of the organization should ultimately own the Information System Security, and should be responsible for the organization's Information System Security Plan and the Security Policy. The risk analysis defined above should also be directed and supported by senior management. The purpose and scope of the analysis needs to be defined by management. It is also essential for senior management to review the outcome of the risk assessment and analysis and act on its findings.

Please note that this is not comprehensive, and will not meet your organization's complete security needs or make your environment secure overnight. It is evident that it is not just technology and tools, but also people and processes that play an important part in information security.

The above guidelines can be applied to any aspect of Information Systems, including Oracle databases, Oracle Applications and Oracle-based systems.

Security versus Functionality versus Complexity

It is well known that the more you secure something, the less functionality is available. A balance always exists between functionality and security, and in the development world, functionality is usually deemed the most important.

As complexity increases, the security requirements and costs increase. An example is Single Sign-On, which allows a user to access all resources in the environment using a single user ID and password. However, Single Sign-On introduces authentication complexity due to interoperability issues. Similarly, PKI or Public-Key Infrastructure needs to ensure integration of digital signatures and certificates, and also other services required for E-commerce.

It is important NOT to impede user productivity when security is being introduced.

Oracle Security Features

Oracle database and applications should be configured using both the basic and advanced features provided by Oracle. This section describes some of these basic and advanced security features. The above guidelines should be applied while analyzing and implementing these features. The features should be tested and verified in your own environments.

Oracle Basic Security Features

1. Oracle's inherent features ensure data integrity by enforcing semantic integrity, referential integrity and entity integrity. This is achieved through the use of primary keys, foreign keys and unique keys on database tables.
2. Oracle provides configurable operations to help protect database integrity. These are rollback, commits, save point, and checkpoint operations.
3. Oracle handles the database concurrency by ensuring row-level consistency using implicit table and row-level locks.
4. Database views permit specific groups or users to see certain information, while restricting others from viewing it.
5. Oracle provides the ability to GRANT system-level and object-level privileges within databases.
6. Oracle provides a two-phase commit for OLTP transactions when databases are clustered. This ensures that a transaction is not complete until all databases receive and reflect this change.
7. The export and import tools of Oracle help in creating logical backups of the database.
8. Oracle provides mechanisms to create physical backups of the database while the database is in use.
9. There are tools available to verify the integrity of the Oracle database and its components.
10. After the Oracle database or tools are installed, the unused products and features should be de-installed and disabled. Also, unused accounts should be locked or dropped, and default account passwords should be changed.

Oracle Advanced Security Features

1. Oracle's standby database feature can be used to create a hot standby database that is in sync with the primary database. This ensures that in case there is a failure with the primary database or if the primary environment is not available, the hot standby database can be activated with minimal or no data loss, and minimum downtime to services. However, maintaining a standby database is expensive, and has additional overhead. Oracle has recently termed this feature as Oracle Data Guard.
2. Database replication can be used to replicate the database across geographical sites in a distributed database system. Replication provides improved performance and increased availability of applications.
3. Oracle provides Single Sign-On with most of its products by using Oracle Internet Directory / LDAP. With Single Sign-On, users have to log in only once to access all system resources and applications.
4. Virtual Private Database (VPD) enables a number of clients to access data stored on a common shared hosted database server while limiting each client to their own data.
5. Secure Application Context enables an application to tailor access control based on the attributes of the database user's session.
6. Oracle Label Security provides a toolkit to build labels and associate the corresponding label security policy with a table or view.
7. Oracle's Recovery Manager (RMAN) facilitates the physical backup and restoration of a database and its components.
8. Oracle provides several features and enhancements to reduce the recovery time frame and eliminate data loss.
9. Oracle Real Application Clusters (RAC) can be used in High Availability solutions, and where scalability superior performance is required. Also, there are several other features within the database that result in high availability. For example, a database table can be recovered from the Recycle Bin with the FLASHBACK TABLE command. Also, database objects can be rebuilt and re-organized online with no impact to service.
10. SQL*Net encryption should be used to prevent snooping while serving data from database servers to web or application servers.
11. Database encryption (using DBMS_OBFUSCATION) methods can be used to encrypt sensitive data like credit card numbers and account numbers stored in databases, preventing visibility to administrators and users alike.
12. Transparent Data Encryption (TDE) uses a second encryption key that is stored in an Oracle Wallet file outside of the database and is therefore much harder to crack. If you got access to the key in the database, you still couldn't decrypt the data, unless you also got access to the other key.

Several of the Oracle Advanced Security features are available only with Enterprise Edition. Please check the Oracle documentation for specific details.

Summary

- Confidentiality, Availability and Integrity are the fundamental principles of an Information Security Plan.

- Security is not a technical issue. Security should be considered as an essential requirement of the business.
- A top-down approach for implementing information security should be used. Where there is uncertainty in terms of implementation, the security policy should be referenced.
- The organization's challenge lies in enforcing and monitoring the security policy.
- Security should be integrated into the planning and development of databases, systems and all related applications.
- Technology plays a very small part; people and processes play the major part in information security.
- Availability is extremely important in business continuity.
- There is no such thing as a 100 percent secure environment. The challenge is in identifying the risks, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.
- Information security can be an actual source of competitive advantage.
- Management support is the most important and essential pieces of a security program.
