



Delaware State University Procedure

Title: Banner Data Security	Administrative Council approval date: 6/28/06
Related Policies and Procedures:	

Introduction

This document examines the current security policy for the Banner database at Delaware State University and considers possible modifications that can be implemented to improve the level of security. The topic of security is a broad one and a complete treatment is beyond the scope of this document. This document will focus on three main areas of security as they relate to the Banner database at the university. The first area concerns user account passwords, how they are selected, maintained and how they affect the security of the database. The second area is system resources and how they can be managed using currently available database system facilities. The last area addressed is the topic of Banner classes and Oracle roles. Classes and roles are used to control user access to database objects and processes.

As other security issues arise, perhaps concerning other enterprise applications, the principles embodied in this document will be applied in resolving them.

Oracle and Banner Background Information

Oracle in this document refers to the database management software provided by the Oracle company. The term Banner refers to the database software written by the SunGard Higher Education company which uses Oracle as the underlying management software.

A special database object known as a profile, is provided by Oracle to help administrators control the use of system resources. System resources include CPU usage, use of system memory, session connect time and session idle time. Within each profile, resource usage limits are defined and when that limit is exceeded Oracle stops further processing. Each database user is assigned to a profile and the usage limits defined are used to control how the user uses the system. Different profiles can be defined to provide different usage characteristics for different groups of individuals. Profiles can also be used to control the management of user passwords.

User database object access is controlled by Oracle using an object called a role. Roles are granted access to database objects such as tables, views and procedures. Users then obtain object access by being granted access to a previously defined role. Access to objects can be granted directly to users without using roles. Roles are provided as a convenient management tool for database administrators.

Access to Banner reports and processes is managed using a concept known as classes. Reports and processes are assigned to classes which are associated with Oracle roles. Classes are then associated with database users to allow access to the underlying system objects required by each of the class processes and reports. Classes are used in a manner similar to Oracle roles to control access to database reports and processes.

Oracle Password Encryption Information

Oracle uses an encryption algorithm that generates a hash string from the concatenation of a user's account code and a selected password. This hash string is then stored in the Oracle database. Easily available password cracker programs are available that can use a brute force attack approach to determine passwords. Studies have shown that with the user code and the hash string, passwords can be determined in a relatively short amount of time for short passwords as the following figures show:

- 10 seconds to calculate all 5-ascii-character-combinations
- 5 minutes to calculate all 6-ascii-character-combinations
- 2 hours to calculate all 7-ascii-character-combinations
- 2,1 days to calculate all 8-ascii-character-combinations
- 57 days to calculate all 9-ascii-character-combinations
- 4 years to calculate all 10-ascii-character-combinations

These figures would seem to suggest that longer passwords provide an added level of security to an Oracle database.

For a complete discussion of this topic, visit the 'www.red-database-security.com' website listed in the **References and Related Documentation** section at the bottom of this document.

Current Security Policy at the University

Database system resources are currently being controlled by a common default user profile. Therefore, each user that accesses the Banner database shares the same profile that controls how system memory is used, how passwords are chosen and how idle connect time is managed. Database administrators now have the same profile as general users, Banner user accounts and outside system auditors. Currently no idle timeout is enforced at the database level. System memory usage and connect time are now not being limited by the default profile.

Passwords are not being controlled by the default user profile provided. Users therefore can choose passwords in a manner that does not conform to any university standard. Passwords are not required to be changed by the profile and a lockout mechanism is not in place to prevent multiple failed login attempts. A check is currently not being made to prevent passwords from being reused.

Oracle roles and Banner classes exist that were created in the mid 1990's when the Banner system was first implemented. They have been modified since then, as requests were received, in an effort to make changes to user access rights. The way in which new access was granted to users was not always consistent with the original design of the system. As employees have moved to different departments or have left the university, the original rights either have not been modified or in some cases have not been removed from the system. The system is therefore in a state where access is not always consistent with the requirements of user positions and some entries exist that should be removed.

Recommended Modifications to the Security Policy

The following recommendations relate to the three security areas discussed in this document. In general, the recommendation is to provide only the access needed by users to perform their work (least access approach) and to secure access to the system through passwords that are geared to the privileges of the user account.

Control of System Resources

Special Oracle Accounts Sessions per User: 2
Connect Time: Unlimited
Idle Time: 30 minutes
Private SGA (memory allocation): Unlimited

Banner Accounts, Sessions per User: 3
DBAs and Developers Connect Time: Unlimited
Idle Time: 30 minutes
Private SGA: Unlimited

Special User Accounts Sessions per User: 2
Connect Time: 1440 minutes
Idle Time: 30 minutes
Private SGA: Unlimited

General User Accounts Sessions per User: 2
Connect Time: 600 minutes
Idle Time: 15 minutes
Private SGA: Unlimited

Passwords

Special System Accounts 12 character password comprised of letters, digits and special characters, expires every 60 days, reuse allowed after 18250 days, grace time of 10 days, lock account after 3 failed attempts

Banner Accounts, 10 character password comprised of letters, digits and DBAs and Developers special characters, expires every 60 days, reuse allowed after 18250 days, grace time of 10 days, lock account after 3 failed attempts

General User Accounts 8 character password comprised of letters, digits and special characters, expires every 90 days, reuse allowed after 18250 days, grace time of 5 days, lock account after 5 failed attempts

Remove hard-coded password references from existing applications

Classes and Roles

Banner Classes

Create a set of standard classes each containing a set of access rights required by a group of Banner users. The access rights should be assigned in a way to provide the minimum rights required by individuals associated with the class. If modifications to the access rights are required, then modify the class rights and the associated users will all be modified.

Oracle Roles

Create a set of standard roles each containing a set of access rights required by a group of Oracle users. The access rights should be assigned in a way to provide the minimum rights required by individuals associated with the role. If modifications to the access rights are required, then modify the role rights and the associated users will all be modified.

Review Banner classes and Oracle roles periodically to ensure that user accounts listed are currently active and that the correct access is associated with each account.

Conclusion

The current security policy in place on the Banner database at the university is inadequate to provide sufficient protection. This document has discussed three areas of security as they relate to the Banner database at the university, the current policy and recommendations of modifications to the security policy to provide better protection to data in the Banner system. Other security issues need to be addressed, in addition to those discussed in this document, that affect the overall security of the database.

See articles in the **References and Related Documentation** section below for further information.

References and Related Documents

<http://soi3.mmtel.ru/books/useoracle8/ch11/ch11.htm>

<http://www.oreilly.com/catalog/orasec/chapter/ch07.html>

<http://www.pcworld.com/resource/printable/article/0,aid,123289,00.asp>

http://www.red-database-security.com/whitepaper/oracle_passwords.html

http://www.oracle.com/technology/products/id_mgmt/pdf/idmwindows_10.1.2_twp.pdf

http://www.oracleanalyzer.com/archives/2004/02/managing_passwo.html