Report Number: C4-10R-03

Guide to the Secure Configuration and Administration of Oracle9iâ Database Server

Network Applications Team
Of the
Systems and Network Attack Center (SNAC)

Authors:
James Hayes, Maj USAF, CISSP
Sheila Christman

Dated: 30 September 2003
Version 1.2

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

SNAC.Guides@nsa.gov

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows versions or operating systems.
- This document may contain recommended settings for the system Registry. Oracle9i can be severely impaired or disabled with incorrect changes or accidental deletions when using a Registry editor (Regedt32.exe or Regedit.exe) to change the system configuration.
- Currently, there is no **undo** command for deletions within the Registry. Registry editor prompts the user to confirm the deletions if **Confirm on Delete** (Regedt32.exe) is selected from the options menu. When a key is deleted, the message does not include the name of the key being deleted. Therefore, check selection carefully before proceeding.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- See Microsoft's web page for the latest changes or modifications to the Windows 2000 operating system and Oracle's web page for Oracle9i.

Acknowledgements

This document is highly dependent upon The Center for Internet Security's (CIS's) *Oracle Database Security Benchmark v1.0*, without which this guide would not be possible. We would like to thank all of the team members that participated in the development of this CIS benchmark document.

Trademark Information

Table of Contents

This Page Intentionally Left Blank

Introduction

Oracle9i is a robust relational database server. It offers many features to control access to database tables and resources. In addition, it will allow administrators to control resource consumption as well as other abilities to provide fine grain control over users who access the server. Oracle9i is supported on many platforms; however, the installation and guidance provided in this document will focus on the Windows 2000 operating system (OS).

This document will describe how to securely configure and administer the Oracle9i Enterprise Edition Database Server (hereafter referred to as Oracle9i) that is part of a Windows 2000 domain, i.e., intranet. This guide must be supplemented with The Center for Internet Security's (CIS's) Oracle Database Security Benchmark v1.0. This benchmark can be downloaded from CIS's website at http://www.cisecurity.org. In addition, selected aspects of the Oracle9i Advanced Security option will be reviewed. The focus of this document is security-relevant information pertaining to the configuration and administration of Oracle9i. For a more in-depth discussion on Oracle security, readers should consult books such as the *Oracle Security Handbook, Oracle Security,* and various security material that can be found at the following Oracle web sites: http://www.oracle.com, http://docs.oracle.com, and http://metalink.oracle.com.

This document is intended for the reader who is already familiar with Oracle9i but needs to understand how to configure and administer the product in a more secure manner. The information presented here is written in a direct and concise manner in deference to this intended audience.

Some Oracle9i security issues, and corresponding configuration and administrative actions are very specific to the way the product is being used. For this reason, it is difficult in some areas to recommend specific, concrete actions. Instead, a summary is offered which describes the concerns and recommends solutions that a user must tailor to his environment.

WARNING: This guide does not address security issues for the Microsoft Windows 2000 operating system that are not specifically related to Oracle9i and its implementation.

PLEASE NOTE THAT THESE DOCUMENTS ASSUME THAT THE READER IS A KNOWLEDGEABLE WINDOWS 2000 ADMINISTRATOR AND ORACLE9I DATABASE ADMINISTRATOR. A knowledgeable Windows 2000 administrator is defined as someone who can create and manage accounts and groups, understands how Windows 2000 performs access control, understands how to set account policies and user rights, is familiar with how to setup auditing and read audit logs, etc. These documents do not provide step-by-step instructions on how to perform these basic Windows 2000 administrative functions – it is assumed that the reader is capable of implementing basic instructions regarding Windows 2000 administration without the need for highly detailed instructions. An Oracle9i Database Administrator should have a similar skill set for Oracle9i.

Getting the Most from this Guide

The following list contains suggestions to successfully configure and administer Oracle9i:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations.
- Perform a complete backup of your system before implementing any of the recommendations in this guide.
- Follow the security settings that are appropriate for your environment.

Commonly Used Names

Throughout this guide, the Windows domain TestDomain.Net will be used in the examples, screenshots, and listings.

WARNING: It is extremely important to replace TestDomain.Net with the appropriate domain for the Windows domain being secured. This domain is not a real domain and has been used for demonstration purposes only.

Chapter 1

Windows 2000 and the CIS Baseline

Oracle9i is a robust relational database server and is supported on Windows 2000 and Windows NT operating systems (OSs). The installation and guidance provided in this document will focus on a member-server in a Windows 2000 domain that is implemented in native domain mode, ie., all client operating systems are Windows 2000. Prior to making any adjustments to the OS, it is strongly recommended that all Windows 2000 service packs be applied and the OS baseline security be configured using the National Security Agency's (NSA's) W2K Server.INF. After OS hardening, install Oracle9i and implement CIS's Oracle Database Security Benchmark v1.0 recommendations. Members of NSA worked in collaboration with CIS by participating on CIS's Oracle Benchmark team. Our efforts, in conjunction with other team members, helped produce the aforementioned document.

Operating System Security

File permissions, registry settings, password usage, user rights, and other issues associated with Windows 2000 security will need to be addressed as they have a direct impact on Oracle9i security. This document will focus on an Oracle9i computer that is a member-server of a domain. The Oracle9i computer will use Windows 2000 authentication for user accounts, i.e., Oracle Advanced Security's (OAS) SQLNET.AUTHENTICATION parameter set to NTS. This method is strongly encouraged over using Oracle's native form of authentication. The advantages gained by this tight coupling are no increased complexity, possibly no security holes due to the addition of security layers, and better performance by eliminating unnecessary overhead caused by additional security and access control layers. The primary disadvantages are poor OS security can often cause poor database security and a possibility exists that unauthorized database access can be obtained through a logged-on, unattended workstation.

Prior to configuring Oracle9i, determine how the server will be used. This document will focus on Oracle9i installed on an intranet. The configuration of Oracle9i directories, files, user accounts and profiles, TCP/IP port connections, etc. will be based on your answers to the following questions:

- Will the server be accessed from the Internet?
- Will Windows 2000 or Oracle9i perform authentication? What type of servers will be accessing the database, e.g. web, application or another database?
- Will the database be used for warehousing, data-mining, online transaction processing (OLTP)?
- Is Microsoft Windows 2000 IPSec used throughout the network infrastructure?
- Does data need to be encrypted between client and server?
- Does data need to be encrypted on the server?
- Will the server need to access data across the network or just locally?
- Will backups take place across the network or locally?

General Guidelines

When installing Oracle9i, the following guidelines are recommended:

- Place the Oracle9i computer where it will be physically secure; i.e., behind a locked door where only authorized users can gain access.
- If the domain where Oracle9i is to be installed requires trust links to other domains, ensure the access granted to domain resources through this trust link is what was intended. It is important to document domain trust relationships and the resource access/permissions associated with the trust. If the server will be accessed from the Internet, consider configuring a DMZ with a web server and a database server. If possible, only store information that is meant for public dissemination on this database server. Also, do not configure trust links back to the internal domain from the DMZ. Sensitive or critical information should be kept on a separate database server within the local domain. Several sources are available on the Internet describing DMZ architectures. The "Microsoft Windows 2000 Architecture Guide" is a good resource for this information and can be found on the www.nsa.gov web site.
- Partition the server so that the Oracle9i files can be installed on a different partition or disk from the OS.
- IP routing is disabled by default and should be left that way. If routing is enabled, it is possible to have data pass from the user's Intranet to the Internet.
- If access to the Oracle9i computer is required from the Internet, install it initially with all incoming traffic blocked at the router or firewall. After complete configuration, allow incoming traffic. This is recommended because once the main Oracle9i installation has taken place, the services are active and connections can take place. This can cause a system compromise before there is time to configure the security of the database server.

Operating System Preparation

A number of steps need to be taken to secure the OS in preparation for securing the Oracle9i server.

- Install Windows 2000 on its own drive or partition and apply the latest W2K service packs. (Note: When installing Oracle9i, it should be installed on its own drive or partition as well.)
- Apply the NSA's W2K Server.INF file.
- Implement steps documented in Section 1 - Host Files of the CIS Oracle Database Security Benchmark v1.0 that pertain to Oracle9i and the Windows OS.
- Disable services listed in Appendix C of the CIS Oracle Database Security Benchmark v1.0 as appropriate.
- It is important to note that Windows Authentication (NTS) will not work for domain authentication when using a local account to run the Oracle services. See OAS - Authentication in Chapter 2 of this document for details on how to configure the Oracle9i services account for NTS.

- Create user groups at the domain level and consolidate these global groups from the domain into local groups on the Oracle9i computer.
    - DBAs, developers, security operators, users, etc. should be put into separate groups. These groups should then be added to local groups on the actual Oracle9i server.
    - Determine if DBAs need to be placed in an Administration group
        - Consider whether or not the DBA should be an ordinary user with appropriate privileges; or
        - should only have Windows local administration privileges; or
        - should have domain wide Windows administration privileges.
- Implement a robust antiviral program and intrusion detection system as part of the security policy for your entire site.

Implement CIS Baseline Oracle Configuration Settings

This guide is heavily dependent on the CIS Oracle Database Security Benchmark v1.0. Implement all Level 1 settings as recommended in the guide. See Section 2 of the Oracle Database Security Benchmark v1.0 for further information regarding Level 1 and Level 2 settings. Level 2 recommendations may be optional in the CIS Oracle Database Security Benchmark v1.0; however, guidance in this document requires that Level 2 recommendations also be implemented. It is strongly recommended that NTS, at a minimum, be implemented for database authentication. If username/password authentication must be used for database access, it is recommended that this authentication process be protected using IPSec ESP mode or the OAS SSL option.

Oracle9i Post-Installation

- If the service account is changed after installation, and the previous account is not deleted, ensure the old account permissions are modified so only required permissions on registry keys, directories and files are granted.
- Ensure that the HTTP Service is disabled.

This Page Intentionally Left Blank

Chapter 2

Network Security

There are various solutions that an administrator can implement to address network security, however, this chapter will focus on using Windows Authentication (NTS), Oracle Advanced Security (OAS) and Windows 2000's IPSec. In terms of OAS, only selected options of OAS will be discussed. Before NTS, OAS, and IPSec can be addressed, configuration of the listener.ora and sqlnet.ora files must be defined.

Applying Security with Firewalls and Routers

As stated in the Oracle Database Security Benchmark v1.0, the default Oracle listener port should not be used. This adds one more hurdle that an attacker may have to go through, i.e., scanning ports to determine what ports are open and then having to determine what service is running on a particular port. This in and of itself is not enough. Mechanisms must be put in place to help prevent connections from unauthorized clients. Firewalls and router ACLs can be used to help prevent connections and port scanning from unauthorized clients. In terms of Oracle9i, the service port number used should be blocked to all unauthorized clients on firewalls and routers. Ideally, if connections need to be made by clients in other network enclaves, then a virtual private network or other form of network separation should be used to connect enclaves. Lastly, implementing an intrusion detection system can provide a layer of security by presenting alerts when known attacks are attempted against the network. Some systems are capable of not only detecting, but also performing defined actions when attacks are detected.

Applying IPSec in Windows 2000 Intranet

If the clients that will be served are all Windows 2000 clients, then IPSec should be considered for network security requirements. Even though IPSec can be applied to specific ports and IPs, such as a listener port, implementing IPSec should be done in the context of the total security requirements of an intranet. Guidance can be found in NSA's "Microsoft Windows 2000 IPSec Guide". Even though confidentiality may not be an issue, and considering the layered approach to defense, IPSec should still be considered for its ability to provide an organization with a trusted computing environment.

IPSec can enable an organization to have a trusted computing environment (not necessarily trusted user environment) through its Authentication Header (AH) service. This service is especially useful to organizations that do not have a requirement for encryption of network data. The main benefit is that only domain computers (trusted) will be able to communicate with one another. For more background on setting up a trusted computing environment, refer to Microsoft's *Ask Us About…Security – December 15, 2001* article.

Using MS Terminal Server to Remotely Administer Oracle9i

There are basically two options available to Administrators who want to remotely administer Oracle9i – administration through a listener or through the use of MS Terminal Services. Administrators wishing to remotely administer their servers using MS Terminal Services should consult NSA's "Guide to Securing Microsoft Windows Terminal Services". In addition to the recommendations presented in the guide, the following should be adhered to:

1. Insall MS Terminal Services in remote administration mode.
2. Do not set the active session limit to "never", unless required. Set a reasonable time period that exceeds the average administration period by three hours. For example, if administration is performed between the hours of 0800 hours and 1700 hours, set the session limit to 12 hours.
3. If only one session is required for administration, set the network tab to only allow one session instead of the default of two.
4. Use IPSec for communication between the administrative workstation(s) and the Windows server hosting Oracle9i.

Multiple Listeners and Listener Security

In the past, the listener has been noted for being susceptible to various types of attacks, so it is important that connections be limited by a firewall and/or other methods to mitigate unauthorized connections. Administrators who do not administer their servers locally or via terminal server may want to consider designating a separate listener specifically for administrative purposes. This administrative listener access should be limited to specific workstations within the domain. It is strongly encouraged that the administrative listener be protected using IPSec ESP or the OAS SSL option, even though there may not be an organizational IPSec policy or encryption policy in place. Another consideration may be that certain clients should be directed to different listeners, e.g., internal users to Listener A outside users to Listener B.

Oracle Advanced Security

This section provides suggested guidance for setting options within OAS. It is recommended, at a minimum, that NTS authentication be set in a Windows environment. Review Appendix A of the CIS Oracle Database Security Benchmark v1.0 to determine if implementation of OAS meets security requirements.

OAS – Authentication

The Windows 2000 version of Oracle9i offers four different methods for external authentication: Kerberos 5, CYBERSAFE, RADIUS, and NTS. The default method of OAS authentication installed on a Windows 2000 server is NTS. The NTS method uses Windows authentication. The advantage of NTS authentication is manageability

of accounts. To allow NTS authentication to interact with the domain controller, the TNS Listener will need to be run using either the LocalSystem account or a Windows domain account that is in the local Administrators group.

In order to force NTS authentication only, the following parameters must be set in the SQLNET.ORA file:

SQLNET.AUTHENTICATION_SERVICES=(NTS)

SQLNET.AUTHENTICATION_REQUIRED=True

Username/password based accounts must still be either locked or deleted.

OAS – Integrity

If integrity of data is a concern, i.e., modification of data during communication between clients and server, and no encryption is required when passing data between server and client, use the AH option within Windows 2000 IPSec. Otherwise, configure the Oracle9i server with the OAS integrity recommendations listed in the Oracle Database Security Benchmark v1.0. Clients should be configured with the same values, except CLIENT should be substituted for SERVER. If IPSec AH or SSL is implemented, OAS integrity does not need to be configured.

OAS – Encryption

If encryption of data is a concern, i.e., confidentiality of data during communication between clients and server, it is strongly encouraged that the ESP option within Windows 2000 IPSec or OAS SSL be used. If this is not practical, configure the Oracle9i server with the options in the example below. Clients should be configured with the same Encryption type and crypto algorithm values and CLIENT should be selected for the Encryption value. All Encryption Seed values for clients and server(s) should be different. OAS allows an Encryption Seed value between 10 and 70 characters. The maximum length seed value is recommended and can be generated using the HTML/JavaScript code listed in Appendix A of this document. If the seeder program is not used, avoid using the following reserved characters in a SQLNET.CRYPTO_SEED value:

> Single quote(‘), double quote(“), space, number sign(#), equal sign(=), right or left parenthesis(()), comma(,), or backslash(\).

If IPSec ESP or OAS SSL is in use, OAS encryption does not need to be configured.

OAS – Server Integrity and Encryption

The following is an example of a SQLNET.ORA file set on a server that uses OAS integrity and encryption:

SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER= (SHA1)

NAMES.DEFAULT_DOMAIN = TestDomain.Net

SQLNET.AUTHENTICATION_SERVICES= (NTS)

SQLNET.AUTHENTICATION_REQUIRED=True

SQLNET.ENCRYPTION_TYPES_SERVER= (3DES168, 3DES112)

SQLNET.ENCRYPTION_SERVER = required

SQLNET.CRYPTO_CHECKSUM_SERVER = required

SQLNET.CRYPTO_SEED = j&o6y$@gTrcW-_+{lopBn5hTrdWE2

Note: the SQLNET.CRYPTO_SEED is for illustration purposes only and a 70-character value is strongly recommended.

OAS – Secure Socket Layer

If an organizational policy for IPSec's ESP cannot be implemented, but confidentiality of communications is required, then SSL is the preferred method for establishing network encryption over the OAS encryption option. In order to configure a server to use SSL, a certificate request must first be made to a certificate authority (CA) and the certificate imported using the Oracle Wallet. The Wallet Manager is used to perform various certificate operations, such as requesting, importing, removing, and exporting certificates, as well as exporting wallets. Upon receipt from the CA, the certificate is imported into the certificate wallet.

Once the certificate has been imported, select Auto Login and ensure that the wallet owner is the same account that is used to run the Oracle services; otherwise, SSL will not work.

Access Wallet Manager by clicking on the following pull-down menu item:

Programs->Oracle-OraHome90->Integrated Management Tools->Wallet Manager

Please note that your Oracle home name may differ. In addition, one must ensure that the CA certificate(s) for both the server's certificate and client certificates (if client authentication is required) are trusted and stored in the server's Oracle Wallet. Trust only those CA certificates that are required and remove all others. In addition, as in Figure 1, clients' TNSNAMES.ORA files should be configured to only allow connections where the server's distinguished name in the certificate can be matched.

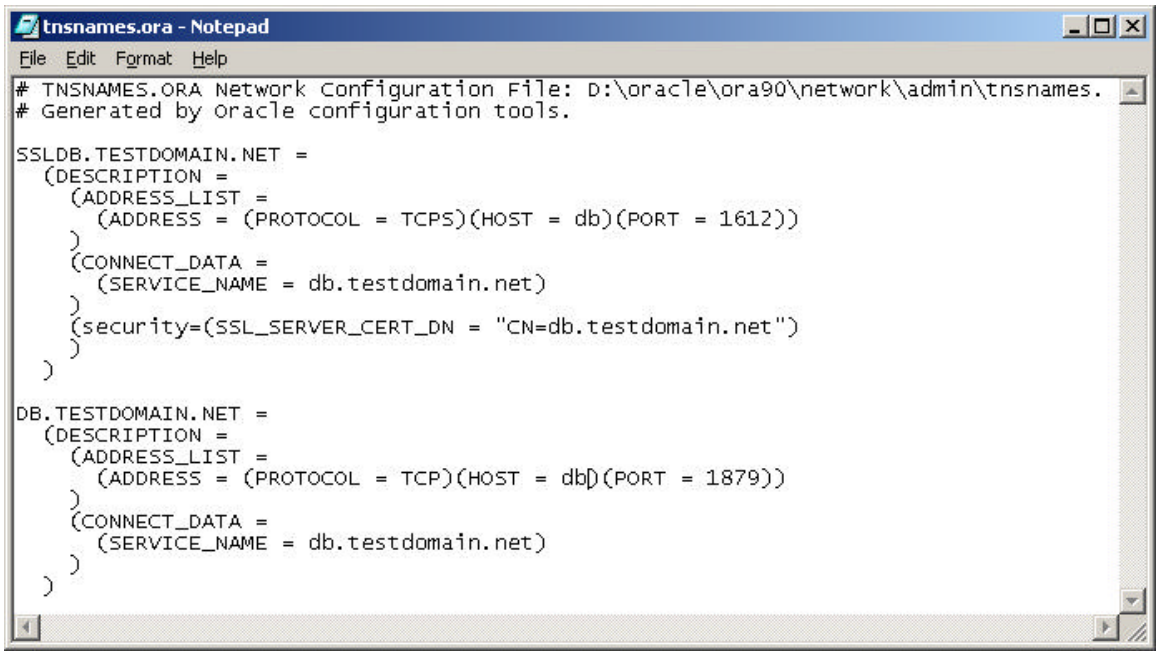
tnsnames.ora - Notepad
File Edit Format Help
TNSNAMES.ORA Network Configuration File: D:\oracle\ora90\network\admin\tnsnames.
Generated by Oracle configuration tools.
SSLDB.TESTDOMAIN.NET =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS)(HOST = db)(PORT = 1612))
)
(CONNECT_DATA =
(SERVICE_NAME = db.testdomain.net)
)
(security=(SSL_SERVER_CERT_DN = "CN=db.testdomain.net")
)
)
DB.TESTDOMAIN.NET =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP)(HOST = db)(PORT = 1879))
)
(CONNECT_DATA =
(SERVICE_NAME = db.testdomain.net)
)
)

Figure 1

References

Christman, S. and Hayes, J., "Guide to the Secure Configuration and Administration of Microsoft SQL Server 2000," http://www.nsa.gov/ .

The Center for Internet Security, "Oracle Database Security Benchmark v1.0", http://www.cisecurity.org/.

"Oracle® Advanced Security Administrator's Guide, Release 9.0.1," June 2001.

"Oracle Advanced Security – Key Management, Data Encryption and Integrity Checking," http://otn.oracle.com/deploy/security/aso/pdf/ASOCrypto_WP.pdf , August 2001.

Greenwald, R., Stackowiak, R., and Stern, J., "Oracle Essentials – Oracle9i, Oracle8i, & Oracle8," O'Reily & Associates, Inc., Sebastopol, CA, 2001.

Heney, W. and Theriault, M., "Oracle Security," O'Reily & Associates, Inc., Sebastopol, CA, 1998.

Newman, A. and Theriault, M., "Oracle Security Handbook," The McGraw-Hill Companies, Inc., Berkeley, CA, 2001.

"Oracle9i Database Administrator's Guide, Release 1 (9.0.1) for Windows," http://otn.oracle.com/documentation/oracle9i_arch_901.html, June 2001.

"Oracle9i Database Installation Guide, Release 1 (9.0.1.1.1) for Windows," http://otn.oracle.com/documentation/oracle9i_arch_901.html, June 2001.

Loney, K. and Theriault, M., "Oracle9i DBA Handbook," The McGraw-Hill Companies, Inc., Berkeley, CA, 2002.

"Oracle9i Network, Directory, and Security Guide, Release 1 (9.0.1) for Windows," http://otn.oracle.com/documentation/oracle9i_arch_901.html, June 2001.

This Page Intentionally Left Blank

Appendix A – Seeder Script

```
<HTML>
<HEAD>
<META http-equiv=”pragma” content=”no-cache”>
<TITLE>(U) SNAC 70 Seed Generator 1.0</TITLE>
<SCRIPT LANGUAGE="JavaScript">
<!--

//*********************************************************
// SNAC 70 SEED Generator 1.0
//
// Author: James Hayes, Maj, USAF
//         Systems and Network Attack Center (SNAC)
//         National Security Agency
// Date:   December 23, 2002
//
//*********************************************************

// This script was developed by the Systems and
// Network Attack Center (SNAC).  Permission is granted
// to use and modify this script provided this notice is
// retained.  Any modification must be clearly
// identified and author and date of modification must
// be noted.
//
// Oracle and SQLNET are either registered trademarks or
// trademarks of Oracle Corporation in the U.S.A. and
// other countries.
//*********************************************************

//*********************************************************
// SOFTWARE IS PROVIDED AS IS AND ANY EXPRESS OR IMPLIED
// WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
// FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED.
// IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY
// DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
// CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
// PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
// USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
// HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
// WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
// (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
// ANYWAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
// ADVISED OF THE POSSIBLITY OF SUCH DAMAGE.
//*********************************************************

//*********************************************************
// This script will allow a user to automatically
// generate a 70 character printable text string that can
```

```
// be used for a SQLNET.CRYPTO_SEED variable.  The
// generator uses both the JavaScript number generator
// and keyboard input.
//**********************Begin Script**********************

function Form_Warning()
{

  msg = "SOFTWARE IS PROVIDED AS IS AND ANY EXPRESS OR IMPLIED\n" +
        "WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE \n" +
        "IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS\n" +
        "FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED.\n" +
        "IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY\n" +
        "DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR\n" +
        "CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,\n" +
        "PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF\n" +
        "USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)\n" +
        "HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,\n" +
        "WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT\n" +
        "(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN\n" +
        "ANYWAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF\n" +
        "ADVISED OF THE POSSIBLITY OF SUCH DAMAGE.";
  alert(msg);

}

function Alert_Notice (form, msg, msg_field)
{

  alert(msg);
  form.seed.focus();
  form.seed.select();
  return;

}

function Convert_to_Hexadecimal(v_base10)
{

// This function will convert the decimal ascii value for a
// printable character to its hex equivalent.

  var v_quotient;
  var v_remainder;
  var v_base16

  v_quotient = Math.floor(v_base10/16);

  v_remainder = v_base10 - (v_quotient * 16);

  if (v_remainder == 10)
  {
    v_base16 = v_quotient.toString() + "A";
```

```
    return v_base16;
  }

  if (v_remainder == 11)
  {
    v_base16 = v_quotient.toString() + "B";
    return v_base16;
  }

  if (v_remainder == 12)
  {
    v_base16 = v_quotient.toString() + "C";
    return v_base16;
  }

  if (v_remainder == 13)
  {
    v_base16 = v_quotient.toString() + "D";
    return v_base16;
  }

  if (v_remainder == 14)
  {
    v_base16 = v_quotient.toString() + "E";
    return v_base16;
  }

  if (v_remainder == 15)
  {
    v_base16 = v_quotient.toString() + "F";
    return v_base16;
  }

  return v_quotient.toString() + v_remainder.toString();

}

function Get_Insert(form)
{

// This function will allow an administrator to select a
// character that will be used to overwrite a character
// that was generated by the JavaScript number
// generator.  For each third of the automated seed that is built,
// the user is asked to replace a character.

  var v_insert_point;
  var v_get_character;
  var v_chr;
  var v_ask_chr = true;
  var v_Auto_Seed;
  var v_good_number = false;
  var v_good_insert = false;
```

```
  var msg

  v_Auto_Seed = form.seed.value;
  msg = "Enter a number between 1 and " + v_Auto_Seed.length;

  while (v_good_number == false)
  {
    v_insert_point = prompt(msg, "");
    if (v_insert_point != null)
    {
      for (var i = 0; i < v_insert_point.length; i++)
      {
        var ch = v_insert_point.substring(i, i + 1);
        if (!(ch >= "0" && ch <= "9"))
        {
          alert("A number was not entered.");
          break;
        }
      }

      if ((v_insert_point >= 1) && (v_insert_point <=
v_Auto_Seed.length))
      {
        v_good_number = true;
      }
    }
    else
    {
      alert("A number between 1 and " + v_Auto_Seed.length + " was not
entered.");
    }
  }

  msg = "Enter one printable character except for a space or one of the
" +
        "following characters: " + ' " ' + " ' " + "# ( ) , = \\";

// Get an allowable printable character from the user.

  while (v_ask_chr)
  {
    v_get_character = prompt(msg, "");
    if (v_get_character != null)
    {
      v_chr = v_get_character.substring(0,1);
      if ((v_chr != '"') && (v_chr != '#') && (v_chr != "'") &&
          (v_chr != '(') && (v_chr != ')') && (v_chr != ',') &&
          (v_chr != '=') && (v_chr != '\\') &&
          (v_chr >= '!') && (v_chr <= '~'))
      {
        return v_Auto_Seed.substring(0, v_insert_point - 1) +
               v_get_character.substring(0,1) +
```

```
              v_Auto_Seed.substring(v_insert_point,
v_Auto_Seed.length);
      }
    }
  }
}

function Generate_Seed(form)
{

// This function will use the JavaScript Math.random function
// to help generate a random decimal number which represents
// the ascii value for a printable character, i.e.,
// auto-keyboard.

  var v_seedsize = 70;
  var v_Auto_Seed = "";
  var v_ascii;
  var v_base16;
  var v_one_third;
  var v_remainder;
  var v_insert_point;

  v_one_third = Math.floor(v_seedsize/3);

  while (v_Auto_Seed.length < v_seedsize)
  {
    v_ascii = Math.floor(Math.random() * 126);

// Screen out printable and nonprintable characters that can cause
problems.

    if ((v_ascii != 34) && (v_ascii != 35) && (v_ascii != 39) &&
        (v_ascii != 40) && (v_ascii != 41) && (v_ascii != 44) &&
        (v_ascii != 61) && (v_ascii != 92) &&
        (v_ascii >= 33) && (v_ascii <= 126))
    {
      v_base16 = Convert_to_Hexadecimal(v_ascii);
      v_Auto_Seed = v_Auto_Seed + unescape("%" + v_base16);

// After each third of the string is built, have the user enter a
// character to replace a randomly generated character.

      if ((v_Auto_Seed.length -
          (Math.floor(v_Auto_Seed.length/v_one_third) * v_one_third) ==
0) &&
          (Math.floor(v_Auto_Seed.length/v_one_third) != 0))
      {
        form.seed.value = v_Auto_Seed;
        v_Auto_Seed = Get_Insert(form);
      }
    }
  }
```

```
  form.seed.value = v_Auto_Seed;
  msg = "Success!  Copy the seed and place it in the sqlnet.ora file
or\n" +
        "enter the seed value via the Oracle GUI in the Encryption Seed
field.\n" +
        "Use a different seed for each client's/server's
SQLNET.CRYPTO_SEED " +
        "parameter.";
  Alert_Notice(form, msg, "Seed");

}

function Clear_Form(form)
{

  form.seed.value = "";

}

function Get_Help()
{

  msg = "1. The seeder will prompt you three times to enter a number\n"
+
        "and a character value.  Each time that you are prompted\n" +
        "for a number or character enter the requested\n" +
        "information with the type and range of value you are being\n"
+
        "prompted to enter.\n" +
        "\n" +
        "2. When you are prompted to enter a character, do not \n" +
        "enter the following reserved characters:\n" +
        "\n" +
        "                    single quote\n" +
        "                    double quote\n" +
        "                    space\n" +
        "                    number sign\n" +
        "                    equal sign\n" +
        "                    right or left parenthesis\n" +
        "                    comma\n" +
        "                    backslash\n" +
        "\n" +
        "3. After you have completed the seed, copy\n" +
        "the highlighted seed value and set the \n" +
        "SQLNET.CRYPTO_SEED parameter with this value in the\n" +
        "SQLNET.ORA file or the OAS GUI.";
  alert(msg);

}
//************************End Script**********************
// -->
</SCRIPT>
```

```
</HEAD>
<BODY onLoad="Form_Warning()">
<CENTER>
<H1>UNCLASSIFIED</H2>
<BR>
<BR>
<H2>Seed<BR>Generator</H2>
</CENTER>
<P>
<FORM METHOD=POST>
<TABLE ALIGN=CENTER>
<TR>
<TD ALIGN=CENTER>
<INPUT TYPE="text" NAME="seed" SIZE=70>
</TD>
</TR>
<TR>
<TD>
 <BR>
</TD>
</TR>
<TR>
<TD ALIGN=CENTER>
<INPUT TYPE="BUTTON" VALUE="     Auto Seed
    " onClick=Generate_Seed(this.form)> 
<INPUT TYPE="RESET" VALUE="     Clear Seed
   " onClick=Clear_Form(this.form)>
<INPUT TYPE="BUTTON" VALUE="  Instructions  "
onClick=Get_Help()>
</TD>
</TR>
<TR>
<TD>
<BR><BR>Click on the <B>Auto Seed</B> button to begin the generation
process.<BR>
This generator creates a 70 character seed value suitable for Oracle
Advanced Security Encryption.
</TD>
</TR>
</TABLE>
</FORM>
<BR>
<BR>
<CENTER>
<H1>UNCLASSIFIED</H2>
</CENTER>
</BODY>
</HTML>
```