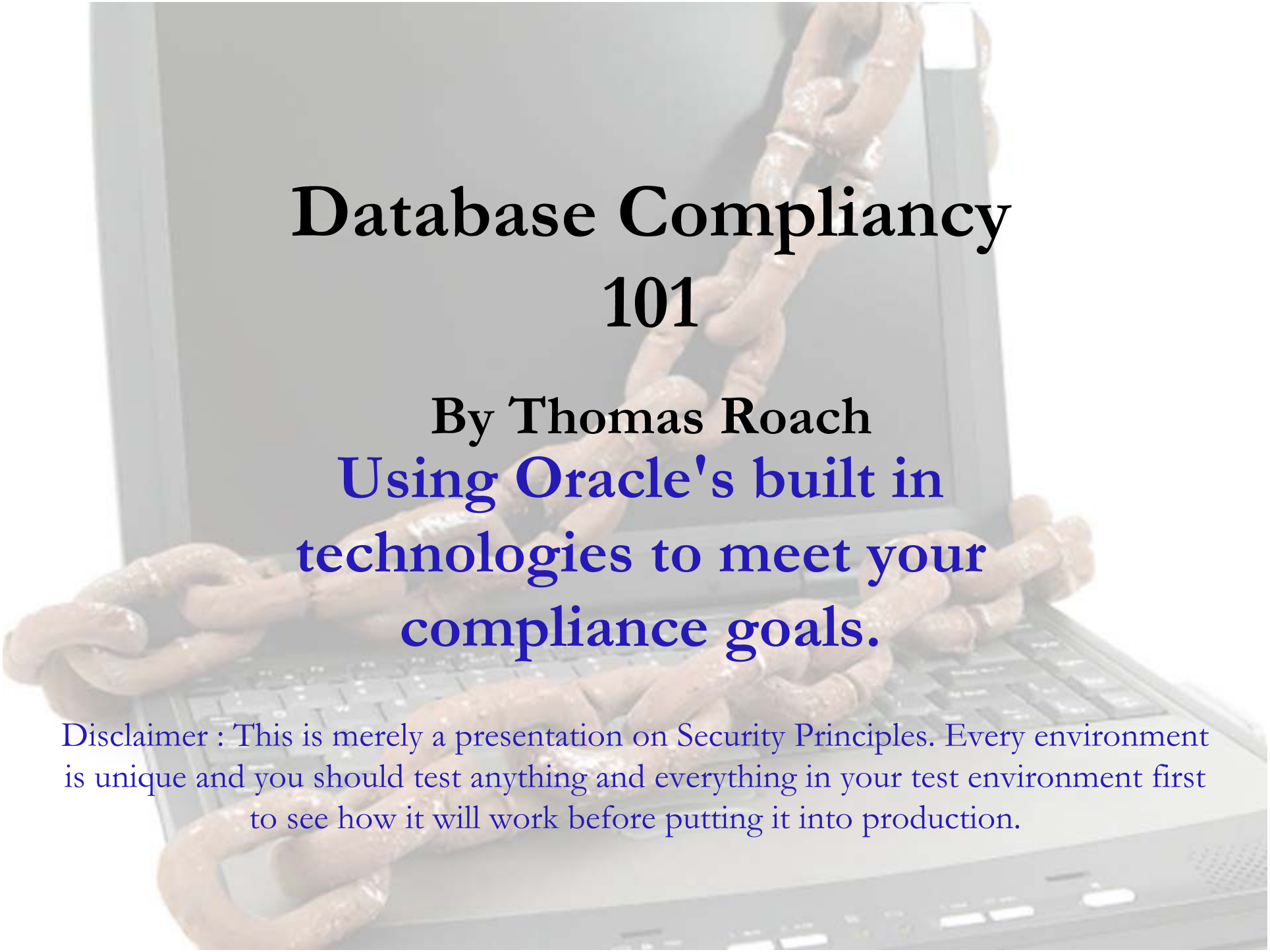


Database Compliancy 101

By Thomas Roach

Using Oracle's built in technologies to meet your compliance goals.

Disclaimer : This is merely a presentation on Security Principles. Every environment is unique and you should test anything and everything in your test environment first to see how it will work before putting it into production.

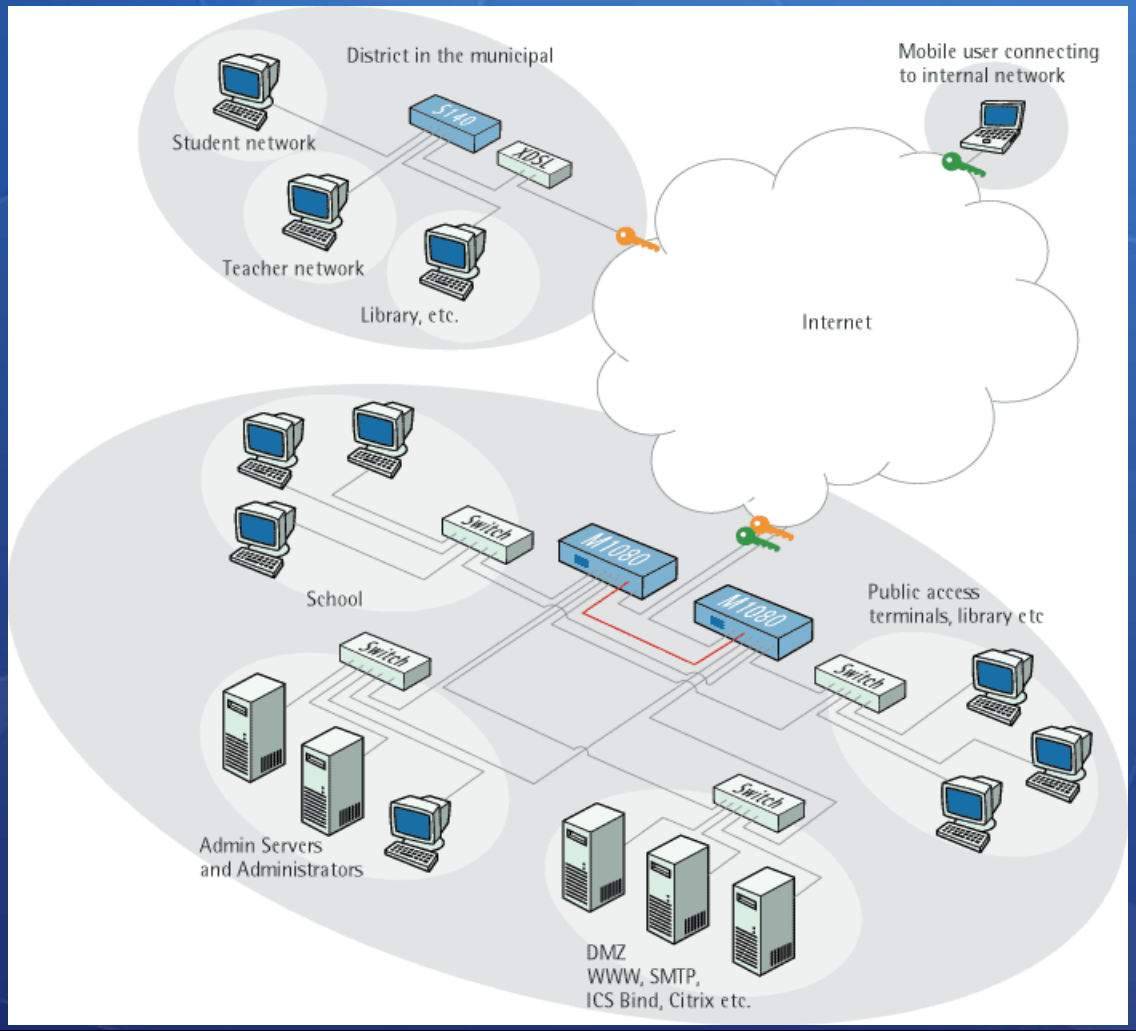
About Me

- Working with Oracle since 2001
- DBA with a local company
- Past President of SOUG
- Practice implementing many of the technologies we will be talking about today

What will we cover?

- Encryption – Network, TDE, DBMS_crypto
- OLS and VPD
- OWM – ASO – FGA
- Compliance Issues : Sarbanes Oxley, HIPAA, PCI, and the Consumer Privacy Act
- Database Vault
- Audit Vault

This is the world we live in



Don’t get caught by a surprise audit!

Consequences of Bad Security

- Bad Publicity
- Media in the parking lot
- Follows paper trail of responsibility
- "You're FIRED!"
- Doesn't look good on the resume

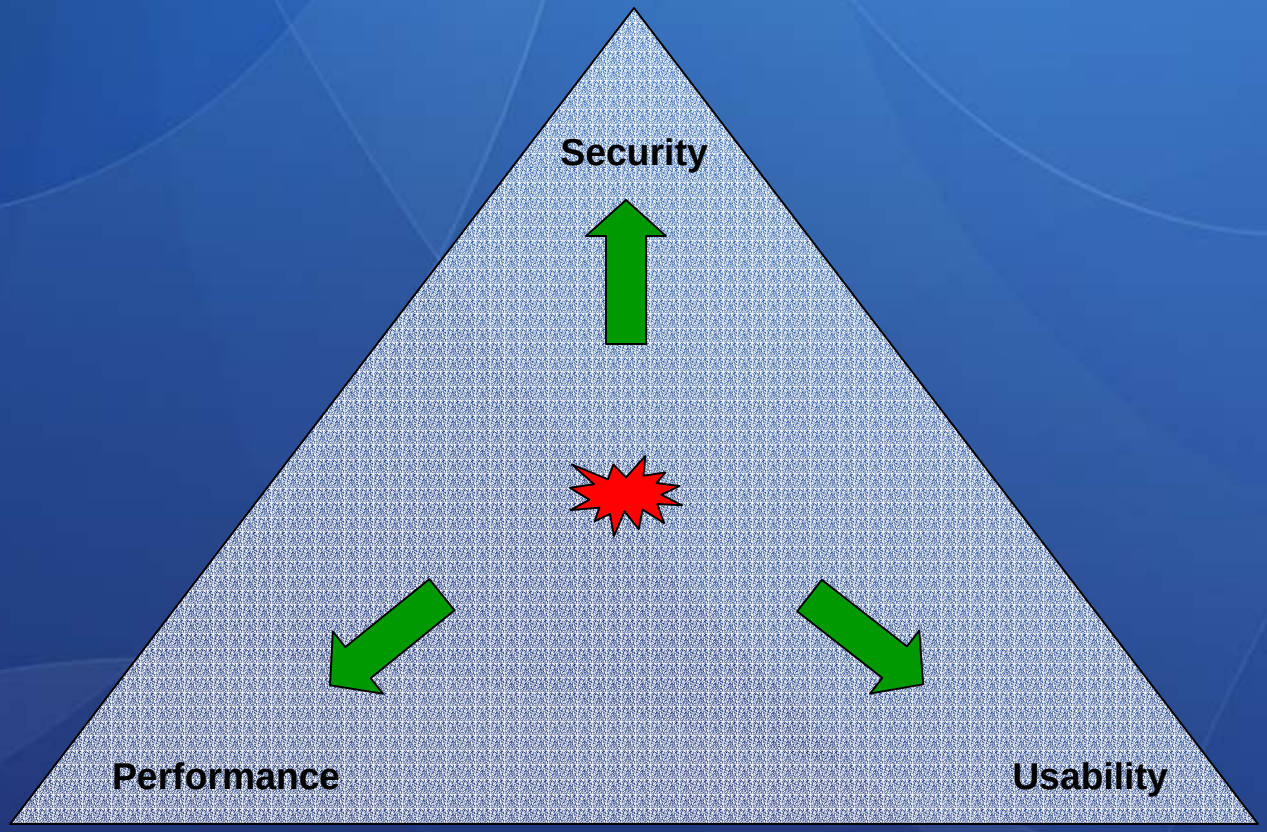
"Securing the database may be the single biggest action an organization can take in proactively defending itself against the myriad of unforeseen hostile intruders."

David Knox - Chief Security Engineer for the Oracle Information Assurance Center in Reston, VA

Strike a Balance

- Security should be practical or it will be self defeating
- Impossible to be 100% secure
- As security increases, usability and performance decrease
- Also, as security increases, so do the costs and complexity

Security – Performance - Usability



Balancing the 3

The Tenets of Security

- Design Security In – Don't bolt it on
- Have multiple layers of security - "Defense in Depth"
- Least Privilege

Just Remember…

Everything Impacts Performance!

DO NOT EVER

- Grant DBA to Public
- Grant System or Object Privs to Public to make an application work
  (Unless you know why and what you are doing, such as Explain Plan)
- GRANT DBA to users (unless they are the DBA)
  If someone does this to make an application work, they are LAZY or "¿No Comprende?".
  Tip - AUDIT

Locking down your database

http://www.oracle.com/technology/pub/articles/project_lockdown/index.html

Project Lockdown

by

Arup Nanda

Enforcing Password Policy

- Use a separate profile for the application user (so the application user's password doesn't expire)
- Should be done on every database (Oracle does not do it by default)
- In order to enable this functionality, run the following script in sqlplus on the server
  `$ORACLE_HOME/rdbms/admin/utlpwdmg.sql`

Modifying utlpwdmg.sql

- Default Function only requires 4 characters – change it to 8
- Has a simple dictionary check, may want to deepen it

```
IF NLS_LOWER(password) IN ('welcome', 'database', 'account', 'user',
'password', 'oracle', 'computer', 'abcd') THEN
```

(For example, tie it into a table of words)

Modifying utlpwdmg.sql cont…

- Add functionality

```
IF NLS_LOWER(password) = NLS_LOWER(username) THEN
```

TO

```
IF INSTR( NLS_LOWER(password), NLS_LOWER(username) )
  != 0 THEN
```

- Now the username cannot be part of the password AT ALL.
- Also checks for 1 digit, 1 letter, and 1 punctuation. Alter to fit requirements.

Modifying utlpwdmg.sql cont…

- Changes the DEFAULT profile

```
ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 60
PASSWORD_GRACE_TIME 10
PASSWORD_REUSE_TIME 1800
PASSWORD_REUSE_MAX UNLIMITED
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_LOCK_TIME 1/1440
PASSWORD_VERIFY_FUNCTION verify_function;
```

- Again, alter to fit YOUR password requirements

Patching / Updates

- Provides the latest security fixes!
- Released every 3 months
- Plan, Test, Production
  Follow your internal change management procedures
- Keep track of all your patch levels (spreadsheet)
- Ensure OPatch is in the path for the oracle user
- Follow the instructions
- `http://www.oracle.com/technology/deploy/security/alerts.htm`

Code Reviews

- Helps find potential security vulnerabilities
- Helps find poorly constructed code
- Helps developers share knowledge and improve productivity!
- Fewer Bugs! (Security and others)
- Ensure rules are followed

Secure Data over an Unsecured Medium

Huh?

What does that mean?

Secure Network and Internet Connections

Secure Backup Media

Firewalls / IDS

- Restricts only the ports that are needed
- Blocks / Allows access from certain network segments
- Can find and block certain attacks (based on signatures)
- Can create logs

Restrict / Allow Network Access

- Use netmgr – General/Access Rights
- Modifies sqlnet.ora
  Adds
  - `TCP.VALIDNODE_CHECKING = YES`
  - `TCP.EXCLUDED_NODES= (HOST1, HOST2 …)`
  - `TCP.INVITED_NODES= (HOST1, HOST2 …)`
- These are mutually exclusive (either exclude or invite / can use wildcards)

Encrypting Network Traffic

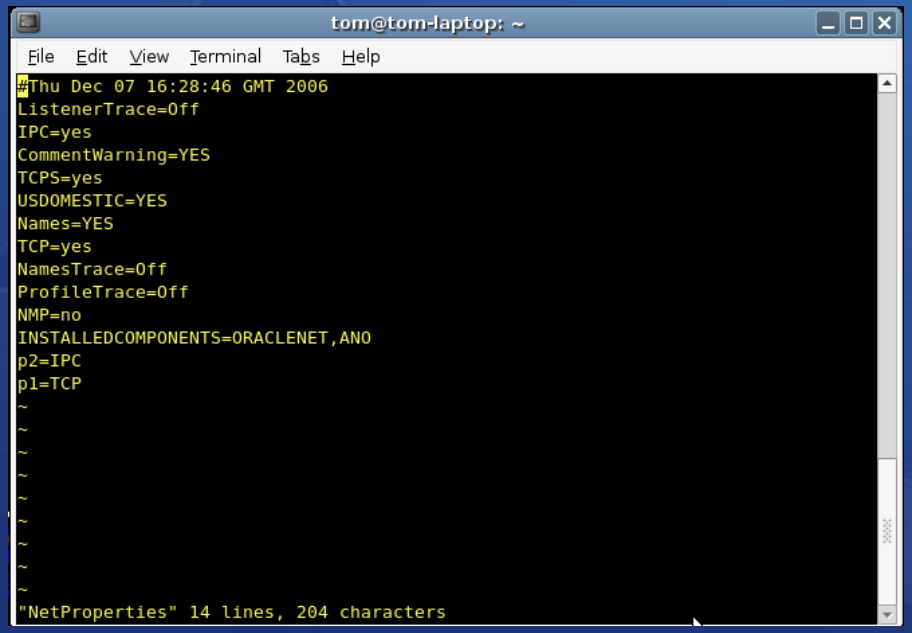
- Use Net Manager (netmgr)
  Try and refrain from editing the sqlnet.ora file directly (other things will break)
- Does not require a certificate
- Seed exists in sqlnet.ora
- Works great with JDBC "Vendor Apps"

Net Manager

- **Must enable ASO.**

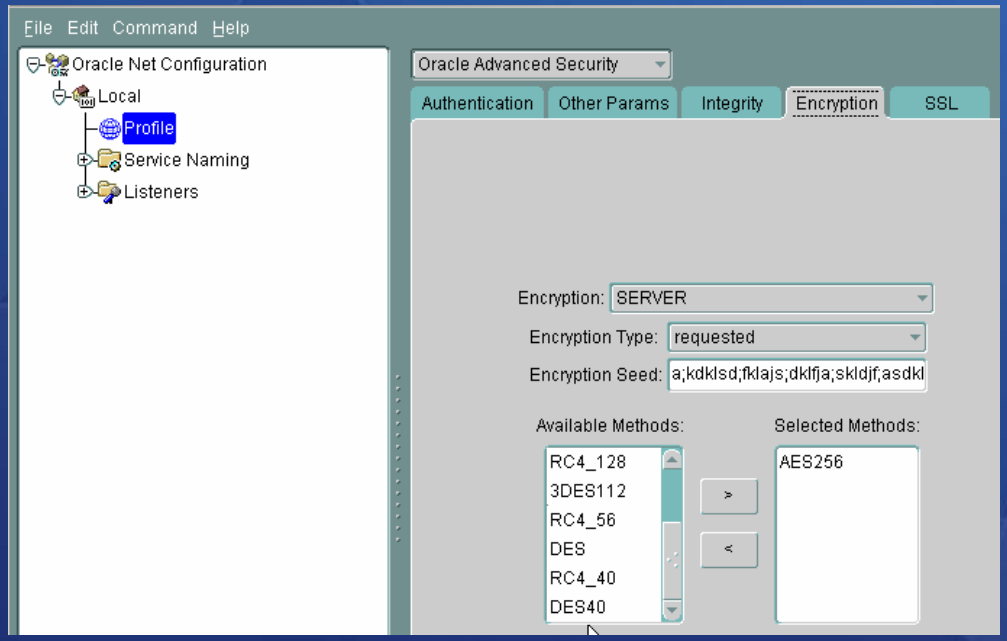
```
vi $ORACLE_HOME/network/tools/NetProperties

INSTALLEDCOMPONENTS=ORACLENET,ANO
```



Net Manager cont…

- Local / Profile / Oracle Advanced Security / Encryption
- Algorithms – AES256, AES192, AES128, 3DES168, 3DES112, RC4_256, RC4_128…

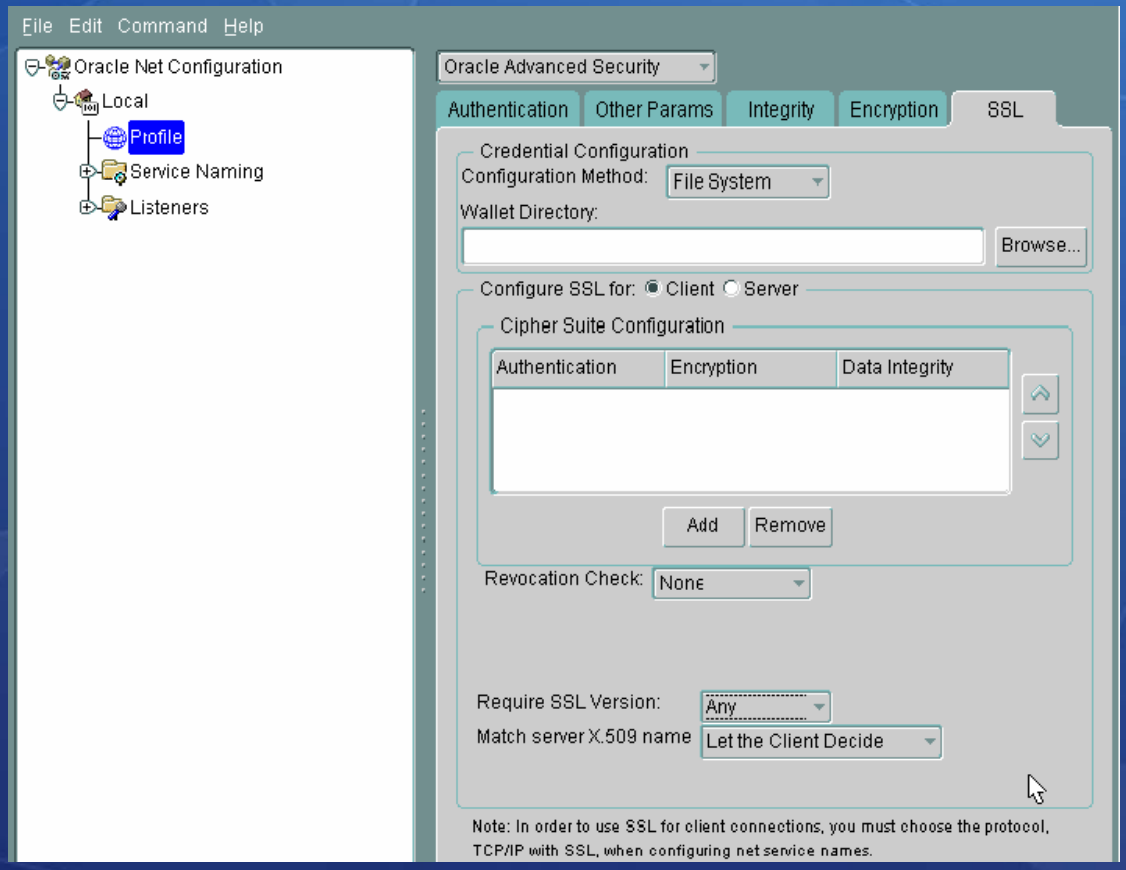


Encrypting with Certificate

- Can do SSL or TLS
- Must create a wallet and set it to auto login on server
- Must also create a wallet on the client and do the same
- Must configure a certificate on the server using wallet manager
- Configure the Listener with netca to use TCPS

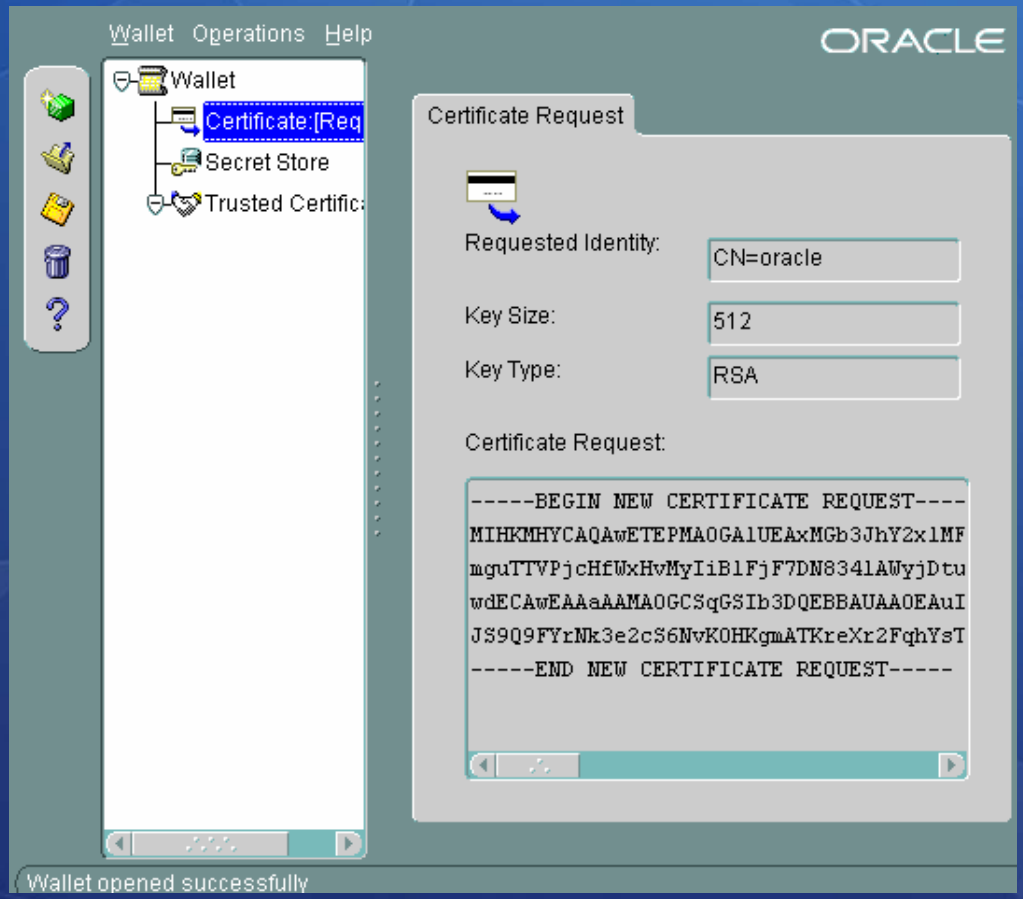
Encrypting with Certificate cont…

$ORACLE_BASE/admin/wallet



Encrypting with Certificate cont…

Oracle Wallet Manager



Encrypting with Certificate cont…

- Update tnsnames on client to use TCPS

```
DB01 =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS)(HOST =
    dbserver)(PORT = 2484)))
   (CONNECT_DATA =
   (SERVICE_NAME = db01)))
SECURITY=
(SSL_SERVER_CERT_DN="cn=db01,cn=OracleContext,c
=us,o=acme")
)
```

- You will then have to update your Listener to use TCPS and restart
  (Make sure you re-register the DB with it "ALTER SYSTEM REGISTER")

For more information refer to Oracle's Advanced Security Guide

RMAN and Exports

- Use the encrypt option in both RMAN and DataPump
- Consider zipping with a password
- 3rd party solutions.

Backing up your data

- If TDE, the blocks and archive logs are already encrypted when backed up.
- Backup Set Encryption

```
CONFIGURE ENCRYPTION FOR [DATABASE | TABLESPACE …]
option.

Please see the RMAN documentation for more details
```

- Consider using Oracle Secure Backup

Encrypting Data at Rest

- It means the data on disk should be encrypted.
- TDE and DBMS_CRYPTO
- Obfuscation Tool Kit

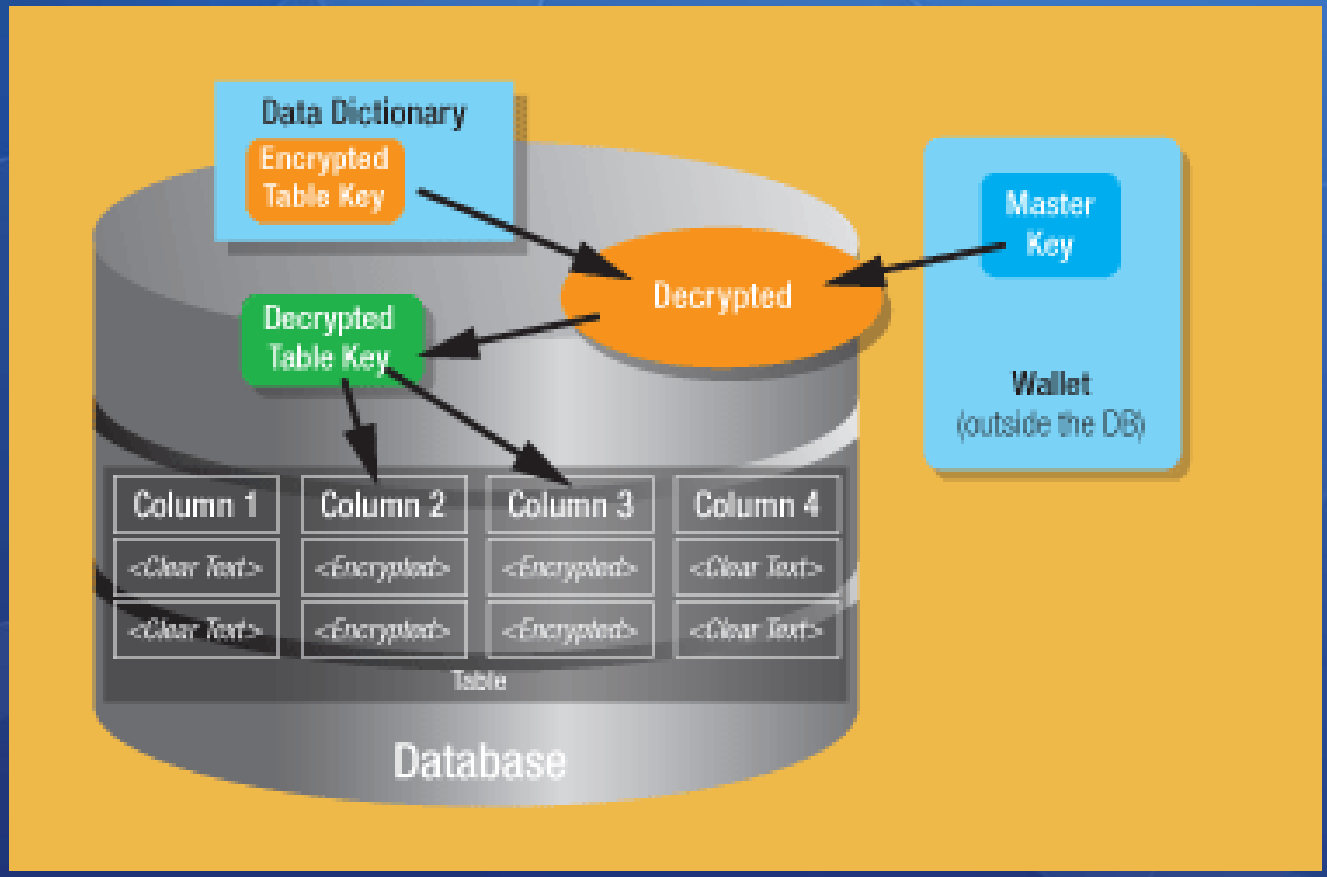
Transparent Data Encryption - TDE

- Presents a way to encrypt data at the file system layer – data files and redo logs / archive logs
- Requires a wallet and for it to be open

```
alter system set encryption key identified by
"mypassword";
```

- Alter Table Modify / Add
- Can be built into new tables
- Transparent to the application and end users " no extra coding!"

How it works


Data Dictionary
Encrypted Table Key
Decrypted
Master Key
Decrypted Table Key
Wallet
(outside the DB)
Column 1
Column 2
Column 3
Column 4
<Clear Text>
<Encrypted>
<Encrypted>
<Clear Text>
<Clear Text>
<Encrypted>
<Encrypted>
<Clear Text>
Table
Database

Defining or Altering a Table

```
CREATE TABLE t
(account number(16) ENCRYPT USING 'AES256' NO SALT,
 merchant_id number (4)
 );

ALTER TABLE t MODIFY (account encrypt using 'AES256');
```

- Account is encrypted using AES256
- NO SALT must be used if you are going to create an index off of it, otherwise the default is SALT
- SALT ensures that 2 of the same values don't appear the same once encrypted

Things to know

- A primary key column can be encrypted, but a foreign key cannot reference it
  - Each table has it's own key
- The overhead is minimal per encrypted column "TEST this for yourself"
- If a key has been compromised, you can re-key

```
alter table t rekey using 'AES256';
```

Things to know cont…

- Great for vendor applications “no code modification
- Great for internal apps that tie into other systems
- Combined with a secure application role, it can be even more secure
- Works at the SQL Layer
- If using Data Pump, then add the following lines to the export job:

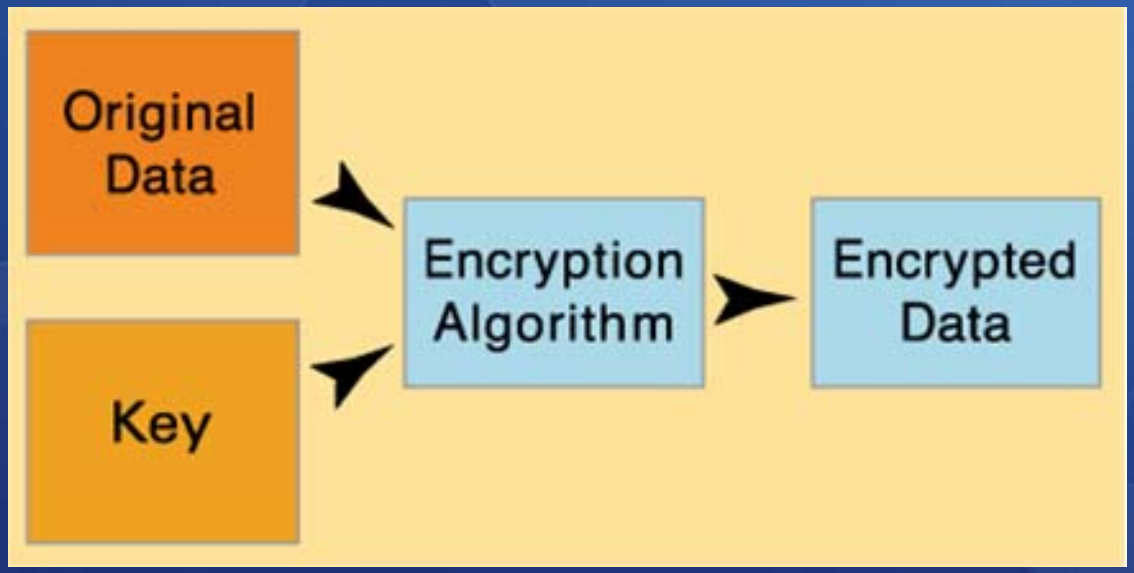
```
ENCRYPTION_PASSWORD=mypassword tables=account_info
```

Things to know cont…

- Log Miner cannot read the data
- If using Data Guard, it must be a physical standby "copy the wallet to the standby"
- Cannot be used with Streams, CDC, Transportable Tablespaces, Materialized View Logs
- Supports 3DES168, AES128, AES192 (default), and AES256

DBMS_Crypto

- The application must manage the encryption via functions/procedures
- How it works



Algorithms

Constant Name	Effective Key Length
ENCRYPT_DES	56
ENCRYPT_3DES	168
ENCRYPT_3DES_2KEY	112
ENCRYPT_AES128	128
ENCRYPT_AES192	192
ENCRYPT_AES256	256

- Just remember, the longer it is = more security / worse performance

Encryption Function

```
create or replace function get_enc_val
(
   p_in     in varchar2,
   p_key    in raw
)
return raw is
   l_enc_val raw (2000);
   l_mod     number := dbms_crypto.ENCRYPT_AES128
                     + dbms_crypto.CHAIN_CBC
                     + dbms_crypto.PAD_PKCS5;
begin
   l_enc_val := dbms_crypto.encrypt
      (
         UTL_I18N.STRING_TO_RAW
            (p_in, 'AL32UTF8'),
         l_mod,
         p_key
      );
   return l_enc_val;
end;
```

Decryption Function

```
create or replace function get_dec_val
  (
     p_in    in raw,
     p_key   in raw
  )
  return varchar2
  is
     l_ret     varchar2 (2000);
     l_dec_val raw (2000);
     l_mod     number := dbms_crypto.ENCRYPT_AES128
                       + dbms_crypto.CHAIN_CBC
                       + dbms_crypto.PAD_PKCS5;
  begin
     l_dec_val := dbms_crypto.decrypt
        (
           p_in,
           l_mod,
           p_key
        );
        l_ret:= UTL_I18N.RAW_TO_CHAR
                     (l_dec_val, 'AL32UTF8');
             return l_ret;
  end;
```

More information

- It is very powerful
- You can store keys in tables, thumb drives etc… to meet your security needs
- Highly customizable and requires coding
- You must have your own key management
- For more information, please visit this wonderful article by Arup Nanda at http://www.oracle.com/technology/oramag/oracle/05-jan/o15security.html
  * I used my code examples and pictures for DBMS_crypto from the above article

Separation of Duties

- Rather than grant DBA to DBA's, have one manage the database and the other manager users.
- Create different roles.
- Consider OLS, VPD, Database Vault

Oracle Database Vault

- Out of the box solution
- Takes the ability of the DBA from seeing sensitive data
- Puts security in the hands of someone else

Requirements

- Separate Product
- Oracle Database 10.2.0.3
- Linux, Windows, Solaris (SPARC)
- Can download at otn.oracle.com
  For more information, visit
  http://www.oracle.com/technology/deploy/security/database-security/database-vault/index.html

Oracle Label Security

- Row level security
- Powerful and makes it easy to create, deploy, maintain fine-grained access control
- Must be licensed and only works with EE
- Use Oracle Policy Manager to manage OLS graphically
- Built on Virtual Private Database toolkit and requires no programming whatsoever

How does it work

- It mediates access to rows in database tables based on a label contained in the row
- Set user label authorizations and privileges
- Apply Oracle Label Security policy to tables and schemas
- Each session is associated with a label
- Label acts as a hidden predicate to all queries for the session - transparent

What problems does it solve

- Hosting Environments
- Control access by means of sensitivity levels, access categories, and user groups
- Multiple organizations accessing a central eBusiness app or Data Warehouse
- Data can be labeled with an “opt-out”
- Database and underlying schemas and database objects (tables) can be shared

Installation requirements

- Must install the Oracle Label Security Option
- Use dbca to configure database options to add OLS
- Then use Oracle Policy Manager to setup and configure OLS
  Please visit this link for detailed install instructions with screen shots
  http://www.oracle.com/technology/obe/obe10gdb/install/lsinstall/lsinstall.htm#o

Virtual Private Database

- Also known as Fine Grained Access Control
- Is included without additional licensing costs
- Coding has to be done but provides more functionality than OLS.
- Can also be combined with OLS

How does it work

```
select * from accounts;
```

VPD REWRITES TO

```
select * from accounts
where user_name = 'SCOTT';
```

You create policy functions

Use dbms_rls package

Policy Types

- Dynamic Policies
  - Only allow a user to bottom 50% of accounts
  - Based on anything that needs to be determined at run time
- Static Policies
  - Only allow access from certain hosts / network segments
  - Only allow access at certain times

Please visit http://www.oracle.com/technology/pub/articles/10gdba/week14_10gdba.html for information on how to setup and configure

Auditing

Who?

Did What?

When?

Where?

Auditing

- Find out who accessed what
- What kind of operation did they perform
  - DDL (CREATE, ALTER & DROP of objects)
  - DML (INSERT UPDATE, DELETE, SELECT, EXECUTE).
  - SYSTEM EVENTS (LOGON, LOGOFF etc.)
- Stored in SYS.AUD$
  - DBA_AUDIT_EXISTS
  - DBA_AUDIT_OBJECT
  - DBA_AUDIT_SESSION
  - DBA_AUDIT_STATEMENT
  - DBA_AUDIT_TRAIL
  - DBA_OBJ_AUDIT_OPTS
  - DBA_PRIV_AUDIT_OPTS
  - DBA_STMT_AUDIT_OPTS

Installation / Configuration

Set "audit_trail = true" in the init.ora file.

Run the $ORACLE_HOME/rdbms/admin/cataudit.sql script while connected as SYS.

```
CONNECT sys/password AS SYSDBA

AUDIT ALL BY userid BY ACCESS;

AUDIT SELECT TABLE, UPDATE TABLE, INSERT TABLE, DELETE TABLE
   BY userid BY ACCESS;

AUDIT EXECUTE PROCEDURE BY userid BY ACCESS;
```

You will want to keep a close eye on your SYS.AUD$ table as it will grow in size. For more information please see http://www.oracle-base.com/articles/8i/Auditing.php

Things you may want to know

- Good idea to audit when users log on and off the system "AUDIT SESSION;" Implement via triggers
- Know who logged in (Application)
- Figure out where you will store the records, plan for growth, and find out when to purge
- Audit "Failures" too, not just Access

Fine Grained Auditing

- Another level of "Fidelity"
- Capture the exact SQL "Not just who did what, but what did they do?"
- Audit when certain conditions met "behaves like an Intrusion Detection System" - Boolean
- Event Handling "Alert administrator" – trip wire.

Enabling

- Different than regular auditing – does not use an initialization parameter to turn on or off

```
BEGIN
DBMS_FGA.add_policy
            (object_schema    => 'TOM',
             object_name      => 'EMP',
             policy_name      => 'Example',
             audit_condition => 'ENAME != USER');
END;
/
```

Reviewing

- Audit Records are stored in SYS.FGA_LOG$
- DBA_FGA_AUDIT_TRAIL is the Data Dictionary View
- DBA_COMMON_AUDIT_TRAIL view combines regular auditing and FGA
- For more information, please read Oracle Database 10g Security Guide and David Knox's Effective Oracle Database 10g Security by Design

Oracle Audit Vault

- New product that is in the roadmap
- Will enable audit data to be stores in a central, secure location
- Will make audit data impossible to touch
- Fulfill separation of duties (SOD) requirements of SOX and PCI "DBA doesn't control the data"
- Can store audit logs from beyond the database(s) – "OS, Applications, Routers – Firewalls etc"
- Can mine the data and use BI to find patterns

Questions

Thomas Roach

troach@gmail.com

How it works

```
statement := "SELECT * FROM users WHERE name = '" +
   userName + "';“
```

If the input is

```
a' or 't'='t
```

Then it renders this

```
SELECT * FROM users WHERE name = 'a' or 't'='t';
```

What is Vulnerable

- JSP, ASP
- XML, XSL, XSQL
- JavaScript, VBScript (Especially client)
- VB, MFC, and other ODBC tools and APIs
- J2EE
- Reports, Discoverer, Oracle Apps
- 3 and 4GL based languages such as C, OCI, Pro*C and COBOL
- Perl, PHP, CGI scripts
- Anything that accesses an Oracle database

Consider this

```
create or replace procedure get_cust (lv_surname in varchar2)
is
        type cv_typ is ref cursor;
        cv cv_typ;
        lv_phone        customers.customer_phone%type;
        lv_stmt         varchar2(32767):='select customer_phone '||
                                         'from customers '||
                                         'where customer_surname='''||
                                         lv_surname||'''';
begin
        dbms_output.put_line('debug:'||lv_stmt);
        open cv for lv_stmt;
        loop
                fetch cv into lv_phone;
                exit when cv%notfound;
                dbms_output.put_line('::'||lv_phone);
        end loop;
        close cv;
end get_cust;
/
```

Look at this

```
SQL> connect dbsnmp/dbsnmp@prd
Connected.
SQL> set serveroutput on size 100000
SQL> exec get_cust('x'' union select username from all_users
   where ''x''=''x');
debug:select customer_phone from customers where
   customer_surname='x' union
select username from all_users where 'x'='x'
::AURORA$JIS$UTILITY$
::AURORA$ORB$UNAUTHENTICATED
::CTXSYS
::DBSNMP
::EMIL
::SYS
::SYSTEM
::WKSYS
::ZULIA
PL/SQL procedure successfully completed.
```

Consider using API's

- Do not give the application user access to underlying data
- Have the application execute stores procedures, packages, and functions
- Pros – very secure
  Cons – take a lot of coding, time consuming

Reiterate

- Be aware of what SQL Injection is
- Do code reviews
- Check for escape characters
- Do not filter on the client side
- Consider API's and removing direct access to underlying tables

Resources – Works Cited

- David Knox – Effective Oracle Database 10g Security by Design "Definitely Buy!"
- Arup Nanda and his many articles on OTN
- Wikipedia
- OTN
- Tapan H Trivedi's presentation to SACOUG
- Oracle Database Security Checklist
- Google!
- Oracle's many manuals
- To anyone I forgot to mention, Thank you