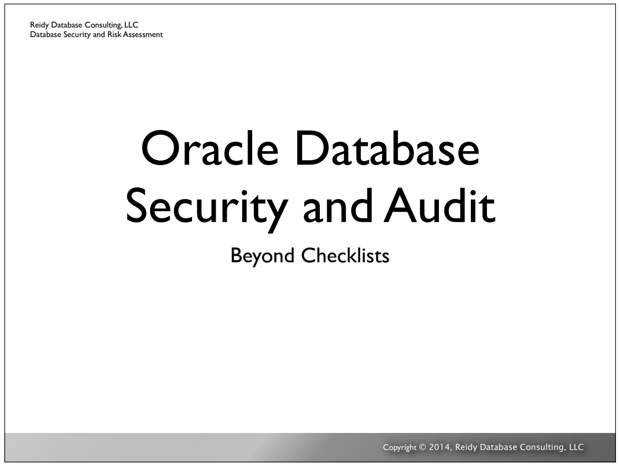
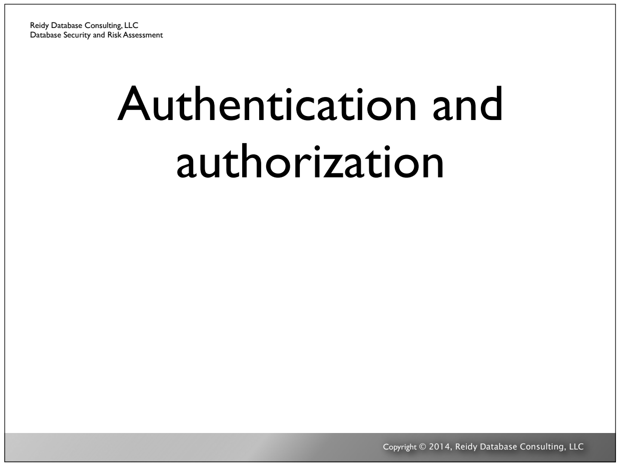
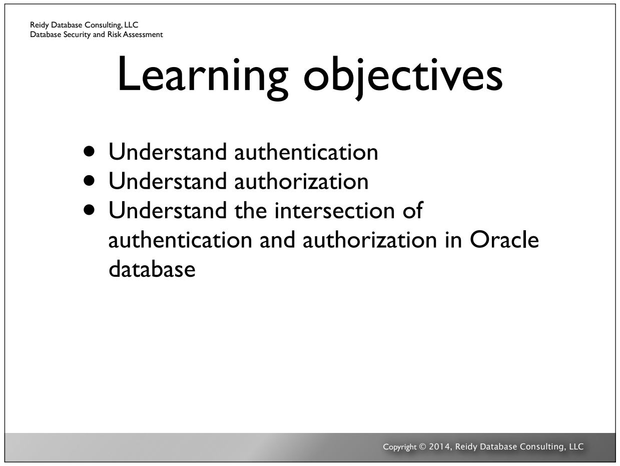


Oracle Database Security and Audit

Beyond Checklists

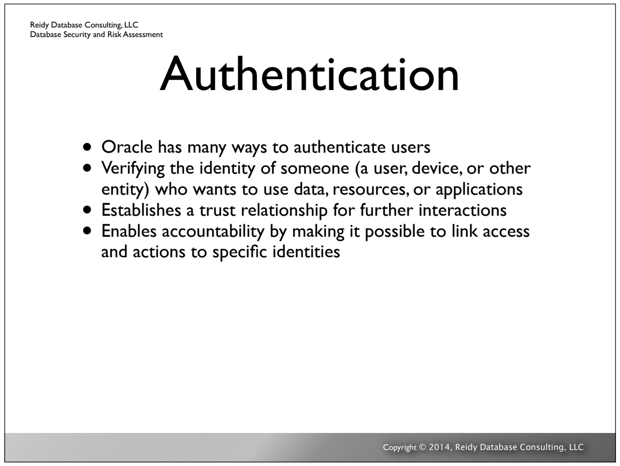


Authentication and authorization



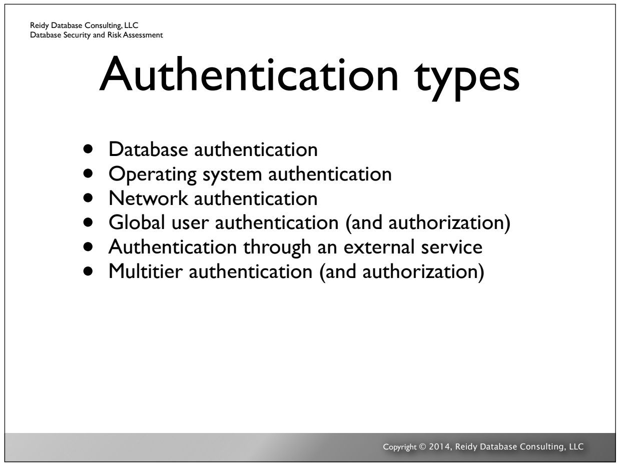
Learning objectives

- Understand authentication
- Understand authorization
- Understand the intersection of authentication and authorization in Oracle database



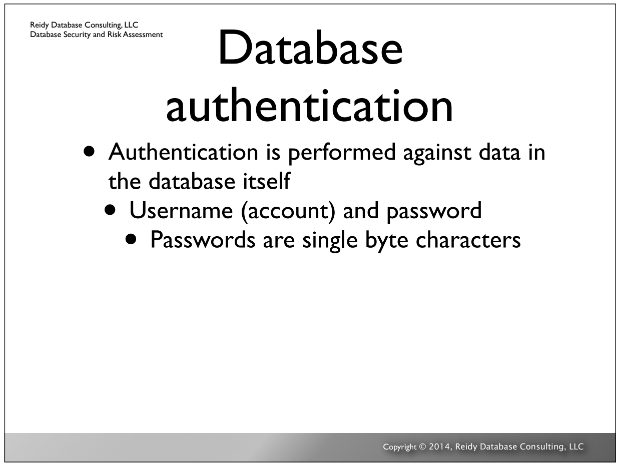
Authentication

- Oracle has many ways to authenticate users
- Verifying the identity of someone (a user, device, or other entity) who wants to use data, resources, or applications
- Establishes a trust relationship for further interactions
- Enables accountability by making it possible to link access and actions to specific identities



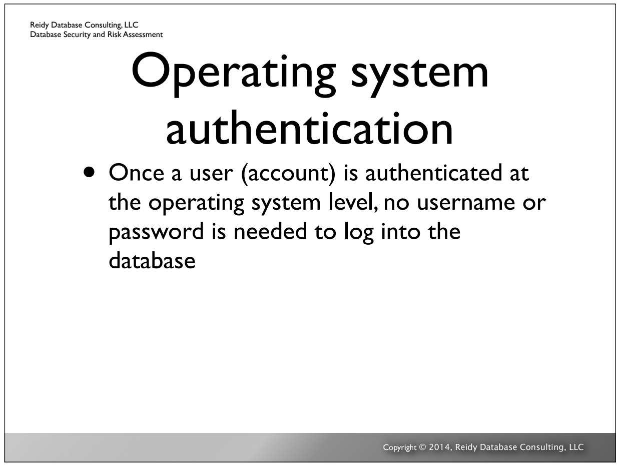
Authentication types

- Database authentication
- Operating system authentication
- Network authentication
- Global user authentication (and authorization)
- Authentication through an external service
- Multitier authentication (and authorization)



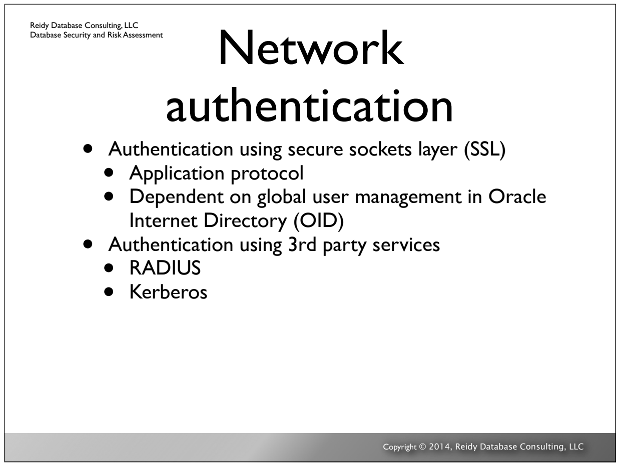
Database authentication

- Authentication is performed against data in the database itself
  - Username (account) and password
    - Passwords are single byte characters



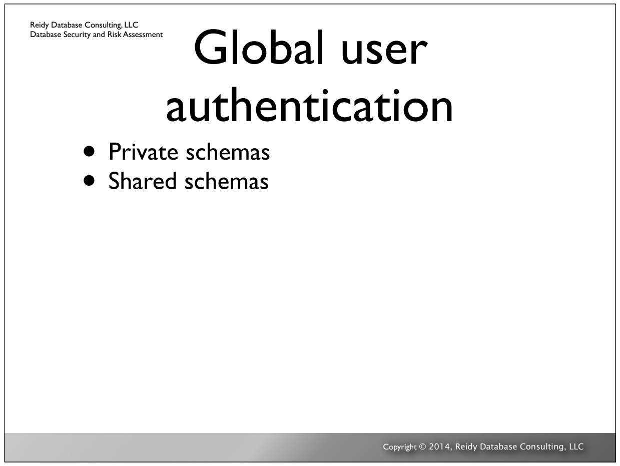
Operating system authentication

- Once a user (account) is authenticated at the operating system level, no username or password is needed to log into the database



Network authentication

- Authentication using secure sockets layer (SSL)
  - Application protocol
  - Dependent on global user management in Oracle Internet Directory (OID)
- Authentication using 3rd party services
  - RADIUS
  - Kerberos



Global user authentication

- Private schemas
- Shared schemas

Authentication through external service

- Oracle database maintains the username (account)
  - External service performs authentication (and password administration)

Multitier authentication

- Oracle Database controls the security of middle-tier applications
  - Limiting their privileges
  - Preserving client identities through all tiers
  - Auditing actions taken on behalf of clients
- Based on trust regions
  - Client authentication performed by the application server (password or X.509 certificate)
  - Application server authenticates the user and itself to the database
  - Database server
    - A authenticates the application server
    - Validates the user exists
    - Verifies the application server has the privilege to connect the user

Database password creation - pre-11g

- Not case sensitive
- One way hash (DES)
- Algorithm
  - Convert username to uppercase version of username (username sys becomes SYS)
  - Convert password to uppercase version of password (password test becomes TEST)
  - Capatilized username and password gets concatinated (username SYS with password TEST becomes SYSTEST)Encrypt (using 3DES algorithm) concatinated value with a (permanent – always the same) secret key
  - Encrypt (using 3DES algorithm) concatinated value with a secret key (this key are the last 8 bytes of the first encryption)
  - The actual password hash value will be the last 8 bytes of the second encryption round, stored in a readable hex representation of these 8 bytes – so 16 characters)

Example: 403888DD08626364

Database password creation - 11g and beyond

- A 10 byte SALT generated by Oracle (looks random)
- Password (case-sensitive) and SALT (10 bytes) value become concatenated
- A SHA1 hash gets generated for the concatenated value
- 11g password hash becomes:
  - “S:” plus
  - <SHA1 hash – readable hex representation> plus
  - <SALT – readable hex representation, 20 characters>

Example: S:7E8E454FCCF9676F15CA93472AADDC2F353BAE2F6C95C519756E150CD727

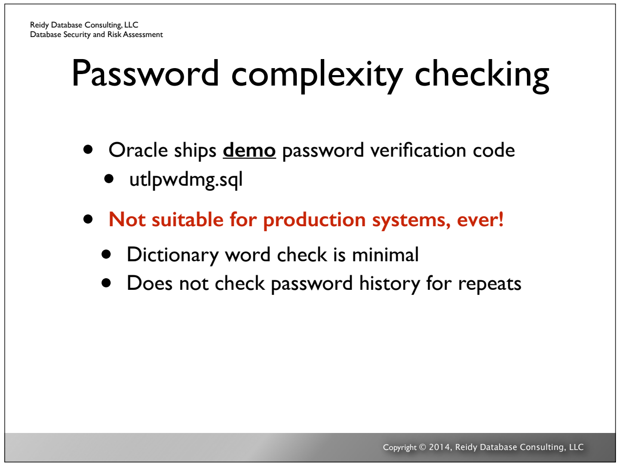
Password protections

- Password encryption during authentication handshake (AES)
- Password failure slow down
- Password complexity checking
- Case sensitivity
- Hashing and salting

Password management policy

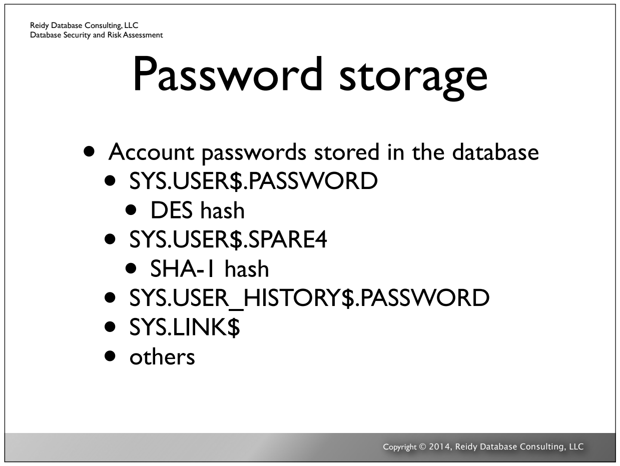
- Password parameters enabled in database profiles
  - All users have a profile
- DEFAULT created when database is created
  - Default (unhardened) parameters

Parameter	Default Setting	Description
FAILED_LOGIN_ATTEMPTS	10	Sets the maximum times a user try to log in and to fail before locking the account.
PASSWORD_GRACE_TIME	7	Sets the number of days that a user has to change his or her password before it expires.
PASSWORD_LIFE_TIME	180	Sets the number of days the user can use his or her current password.
PASSWORD_LOCK_TIME	1	Sets the number of days an account will be locked after the specified number of consecutive failed login attempts. After the time passes, then the account becomes unlocked.
PASSWORD_REUSE_MAX	UNLIMITED	Sets the number of password changes required before the current password can be reused.
PASSWORD_REUSE_TIME	UNLIMITED	Sets the number of days before which a password cannot be reused.



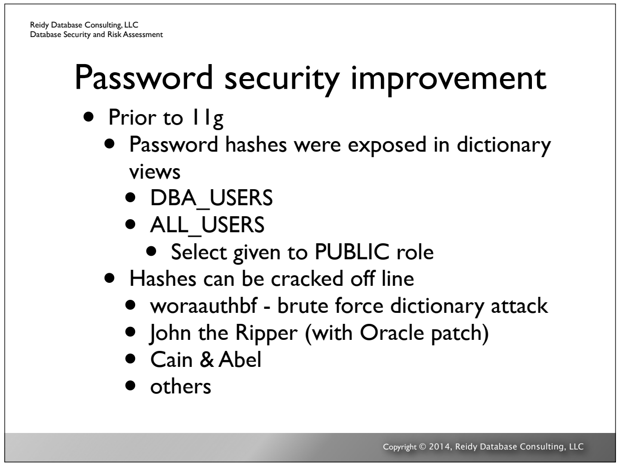
Password complexity checking

- Oracle ships **demo** password verification code
  - utlpwdmg.sql
- **Not suitable for production systems, ever!**
  - Dictionary word check is minimal
  - Does not check password history for repeats



Password storage

- Account passwords stored in the database
  - SYS.USER$.PASSWORD
    - DES hash
  - SYS.USER$.SPARE4
    - SHA-1 hash
  - SYS.USER_HISTORY$.PASSWORD
  - SYS.LINK$
  - others



Password security improvement

- Prior to 11g
  - Password hashes were exposed in dictionary views
    - DBA_USERS
    - ALL_USERS
      - Select given to PUBLIC role
  - Hashes can be cracked off line
    - woraauthbf - brute force dictionary attack
    - John the Ripper (with Oracle patch)
    - Cain & Abel
    - others

Password cracking demos

- Demonstrate two tools to crack passwords
  - Windows based

Legal Disclaimer

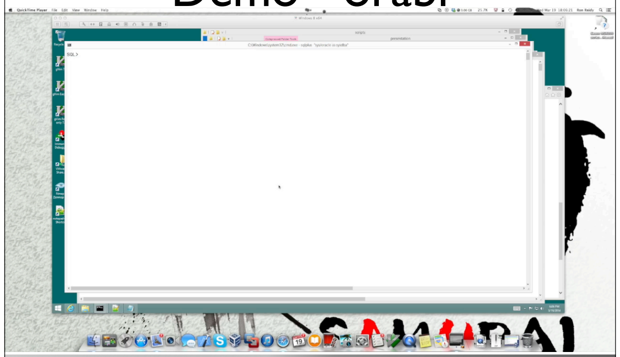
Many organizations have policy against password cracking.

Do not do crack passwords on any systems without written permission from data owners, INFOSEC, etc.

Do not install password cracking tools on your company computers without written consent of your IT department, INFOSEC, etc.

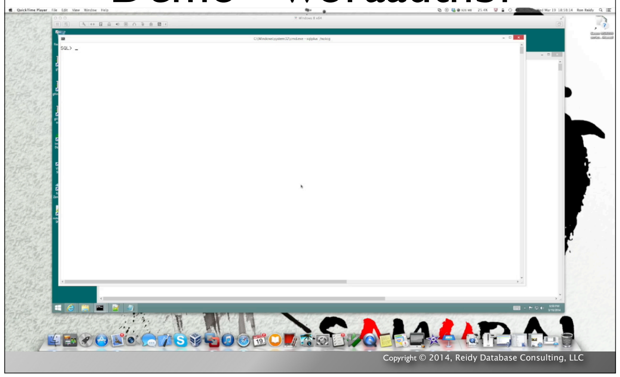
Reidy Database Consulting, LLC assumes no liability for the use of tools at your organization.

Demo - orabf

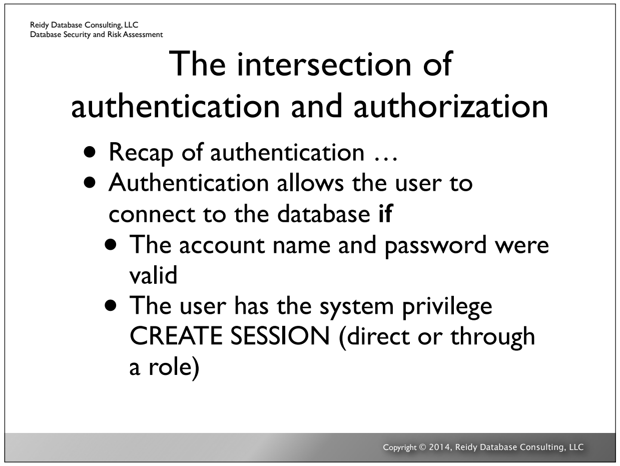

QuickTime Player File Edit View Window Help
Wed Mar 19 18:06:21 Ron Reidy
Windows 8 x64
scripts
presentation
Compressed Folder Tools
C:\Windows\system32\cmd.exe - sqlplus "sys/oracle as sysdba"

```
SQL>
```

Demo - woraauthbf

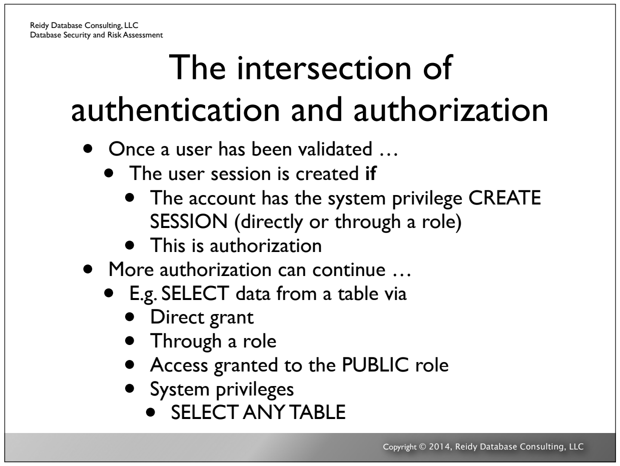

QuickTime Player File Edit View Window Help
Wed Mar 19 18:58:14 Ron Reidy
Windows 8 x64
C:\Windows\system32\cmd.exe - sqlplus /nolog

```
SQL> _
```



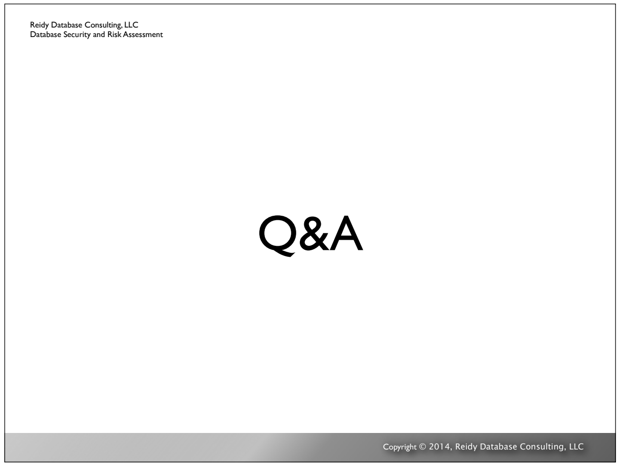
The intersection of authentication and authorization

- Recap of authentication …
- Authentication allows the user to connect to the database **if**
  - The account name and password were valid
  - The user has the system privilege CREATE SESSION (direct or through a role)



The intersection of authentication and authorization

- Once a user has been validated …
  - The user session is created **if**
    - The account has the system privilege CREATE SESSION (directly or through a role)
    - This is authorization
- More authorization can continue …
  - E.g. SELECT data from a table via
    - Direct grant
    - Through a role
    - Access granted to the PUBLIC role
    - System privileges
      - SELECT ANY TABLE



Q&A