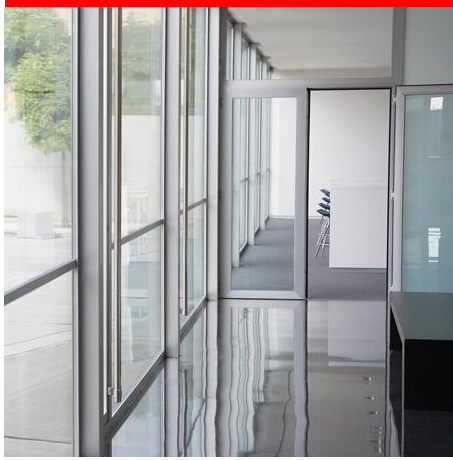

ORACLE®

ORACLE®

High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption

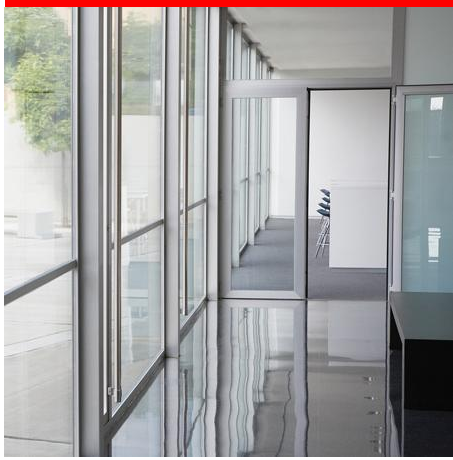
Andreas Becker
Principal Member Technical Staff
Oracle/SAP Development, St. Leon-Rot

Program Agenda



- Oracle Transparent Data Encryption (TDE)
- Oracle Database Vault (DV)

Program Agenda



- Is database security really relevant (for you)?
- Why has database security not been an issue (for you) until now?
- What does “secure” really mean?
- Who is authorized to access data?
- What are the limitations of encryption?
- Is database security “installable”?
- What does “high security” mean for the organization / business processes?
- Summary / Future plans

Is Database Security Really Relevant?

- Database security in the media
  - DOAG NEWS, newspapers, news
  - Internet reports on data theft
    - CDs with lists of German tax evaders
    - Access to personal data about web applications
    - New electronic German identity card
- There are more and more regulations for dealing with data in a secure way
  - National and international regulations (SOX, …)
  - Company-internal regulations

Why Has Database Security Not Been an Issue Until Now?

- There were “more important” problems for a DBA
  - Tuning / Performance (SQL, I/O, Indexes, …)
  - Admin of segments / disk space (VLDB, …)
  - High availability (HA, RAC, Standby)
  - Backup / recovery (RMAN, …)
- Security was not a major issue, even for Oracle
  - Standard passwords (scott/tiger, system/manager, …)
  - Oracle standard users were installed and left open (though not at SAP!)
  - There are some recommendations, but not much more.
  - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts,…, 10.2: CONNECT roles)

Why Has Database Security Not Been an Issue Until Now?

- High security has a price
  - Money: database options DV, ASO require new licenses
  - CPU performance: overhead for encryption / decryption
  - Memory: TDE column encryption (~50 bytes / date)
- High security is awkward
  - Key administration
  - Password administration
  - …
- In addition:
  "My systems are protected by a firewall. So no-one can gain access."
  - What about administrators? → attacks by insiders?

What Does “Secure” Really Mean?

- In general, this refers to the protection of:
  - Data, especially confidential, secret, sensitive data
  - Valuable company data and information
- Such data is …
  - … only secure if only authorized persons have access to the data!
  - … only secure if unauthorized persons do not have access!
  - … insecure if unauthorized persons have access!
  - … secure if authorized people also do not have access?
- Was is meant by “access”?
  - Access means that someone can technically read or change the data, and that this is not prevented, either technically or by some other means, such as authorization checking.

Who is Authorized to Access Data?

- Who is authorized to access data?
  - The SAP application?
  - The SAP application user?
  - The SAP system administrator?
  - The Oracle database administrator?
  - The network administrator? Storage administrator?
- Example: DBA
  - When does the DBA need access to the data? For what kind of administrative task?
  - To correct logical errors
    - False DELETE FROM <table> … WHERE …
      UPDATE <table>… WHERE …
  - To analyze data corruption problems (Oracle errors)
  - Otherwise: NEVER!

What Are the Limitations of Encryption?

- Principle 1: Encryption Does Not Solve Access Control Problems
- Principle 2: Encryption Does Not Protect Against a Malicious Database Administrator
- Principle 3: Encrypting Everything Does Not Make Data Secure

From the Oracle Security Guide

- INSTALL ONLY WHAT IS REQUIRED
- LOCK AND EXPIRE DEFAULT USER ACCOUNTS
- CHANGING DEFAULT USER PASSWORDS
- CHANGE PASSWORDS FOR ADMINISTRATIVE ACCOUNTS
- CHANGE DEFAULT PASSWORDS FOR ALL USERS
- ENFORCE PASSWORD MANAGEMENT
- SECURE BATCH JOBS
- MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES
- ENABLE ORACLE DATA DICTIONARY PROTECTION
- FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE
- …

Follow the Principle of “Least Privilege”

- All users should only receive the authorization they (currently) need to perform their work
  - Example: keys, access cards to firm or specific offices
  - Database users (user/pwd) with roles and privileges
  - Also restricted in terms of duration of access
- In practice: the DBA can do anything (and also see anything)
  - DBA role / SYSDBA authorization
  - Is the DBA role or SYSDBA authorization necessary for every administrative action of the DBA?
  - Does a DBA need access authorization for SAP tables?

Oracle Database Vault

- Database Vault …
  - Restricts the DBA to the authorizations necessary to perform DBA tasks = “Least Privilege Principle”
  - Recommends division of tasks = “Separation of Duty (SoD)”
- Database Vault = “Least Privilege” principle and division of tasks
- DBA regards removal of authorization as a restriction
- Lack of authorization can be a cover / alibi for the DBA
  - Possibility of access to confidential data
  - Murder mystery, Agatha Christie: who had access? Who had the key to the safe?

Oracle Database Vault

- Principle of “division of tasks” (→ Database Vault)
  - Area 1: Database administration → DB administrator DBA
  - Area 2: Database security → Security administrator
  - Area 3: User administration → User administrator
- Division of tasks…
  - Realization of the “least privilege” principle
  - Mutual control or:
  - Make sure that privileges cannot be acquired without proper checks
  - Dynamic assignment of authorization (specific to time and object)
  - “Offshore DBA teams”

Is Database Security “Installable”?

- In principle, yes, but …
- Oracle offers numerous options and features (DV, ASO, …)
- The best installed protection is worthless if it is not used or configured properly!!
  - ASO is installed as standard in SAP
- Example:
  - A domestic alarm system for a house
  - Is useless if the house key is left under the front-door mat or the alarm is deliberately switched off (e.g due to false alarms)
  - Security measures only work if they are correctly deployed.

What Does "High Security" Mean for the Organization?

- Transparent data encryption (TDE) for tablespaces
  - Security administrator: administration of the encryption wallets, wallet passwords
- Database Vault (DV):
  - Division of tasks or introduction of new areas of responsibility (security administrator, account manager)
  - New processes for co-operation between DBA, SecAdmin, AcctMgr
  - Example: export of data / access to data as the DBA only possible on application / with agreement of security administrator
- Auditing
  - Has an audit taken place? What happened to the audited data? How was it evaluated?

What is Data Loss?

- Usual definition of “data loss”:
  - No data loss means that all data is present and correct (that is, not falsified).
  - Protection from data loss achieved by regular backups, application of patches, and so on.
- “Data loss” due to unauthorized access
  - If data falls into the hands of unauthorized persons, this is also a form of data loss (even if the data is present and correct in the system).
  - Results: possibly just harmless or embarrassing but maybe also catastrophic, causing complete business failure

High Security for Your SAP Data with Database Vault and Data Encryption

- Protection from unauthorized access to the data file system (physical access)
  - Encryption of data in data files on physical level with TDE
  - SAP note 974876
- Protection from unauthorized access via the SQL interface
  - Database Vault
  - SAP note 1355140
- BECAUSE YOUR DATA IS VALUABLE!!

Future Plans

- Security is becoming more and more important
- Encryption and division of tasks performed by the system administrators are two important principles for the protection of valuable and sensitive data
- In addition, auditing is becoming more important

SEC_RITY IS NOT COMPLETE WITHOUT U!


ORACLE®

SOFTWARE. HARDWARE. COMPLETE.

Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

Copyright

Copyright