Встроенные средства защиты Oracle9i: новые возможности и опыт применения

Дмитрий Волков

«Инфосистемы Джет»

Oracle9i

БД должна обеспечивать:

- **Хранение, извлечение данных**
- **Возможность гибкого управления данными**

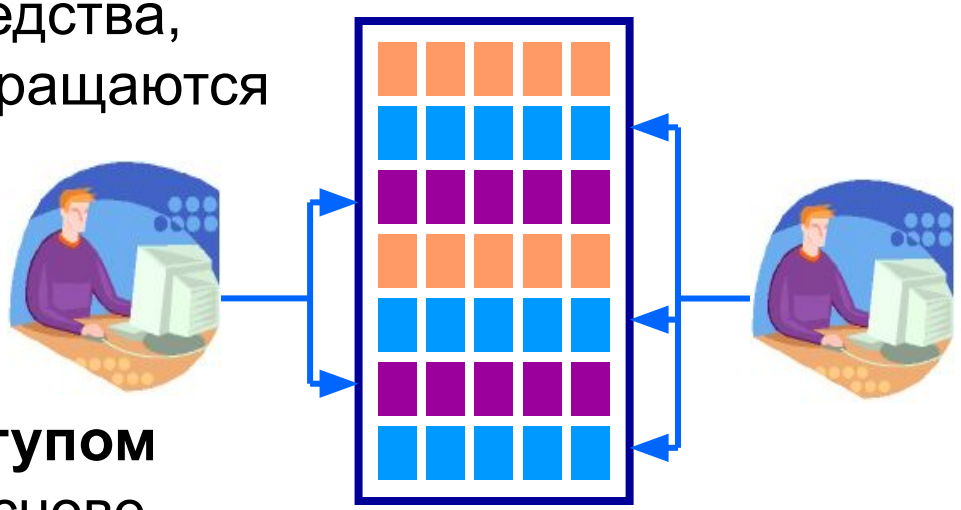
БД должна не дать их украсть !

Основные компоненты обеспечения безопасности

- **Виртуальные частные базы данных** (Virtual Private Database, VPD)
- **Метки безопасности** (Oracle Label Security)
- **Защита выделенных данных** (Selective data encryption)
- **Расширенный аудит** (Extensive auditing)

Виртуальная частная база данных

Пользователи видят только те данные,
к которым они имеют доступ,
вне зависимости от того средства,
с помощью которого они обращаются
к базе данных
(sqlplus, Oracle forms,
MS Office - via odbc)

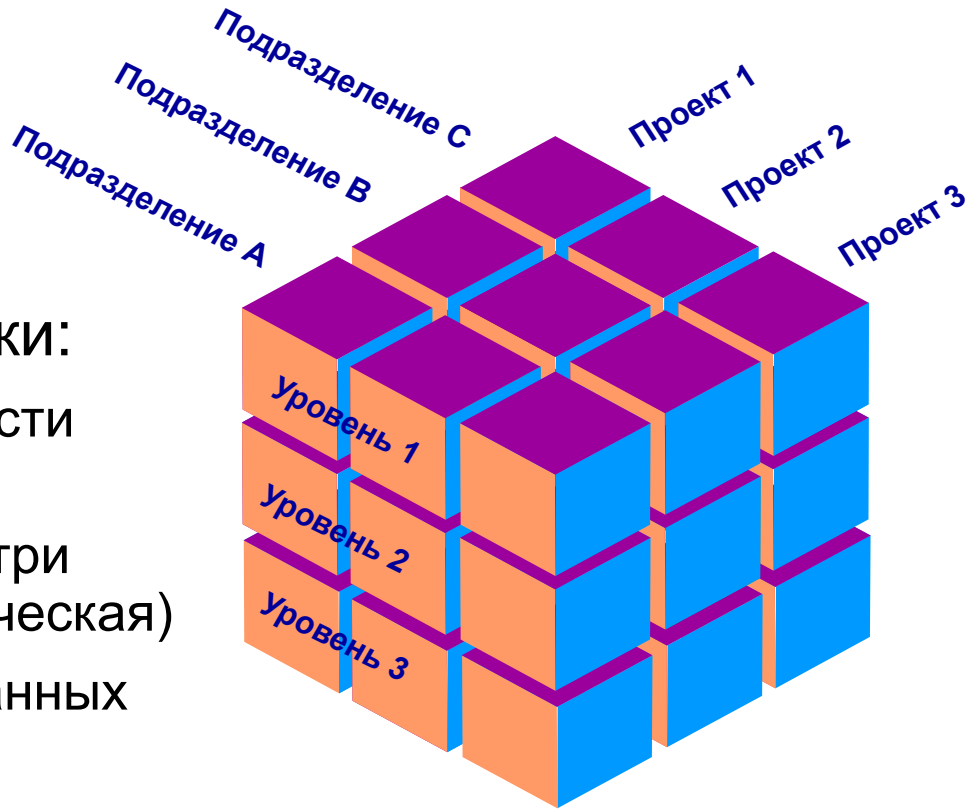


Функции управления доступом
выполняет сам сервер на основе
заданных для него правил вычисления фильтра

Select * from emp → **Select * from emp where dept_no = Sys_context ('emp', 'dept_no')**

Метки безопасности

- Управление доступом на основе меток:
  - пользователей
  - данных



- Классификационные метки:
  - уровень конфиденциальности (иерархический)
  - категория, разделение внутри одного уровня (не иерархическая)
  - группа, принадлежность данных (иерархическая)

Метки безопасности

Oracle9i Release 2 OLS

Метка пользователя:
Конфиденциально : проект 1:бухгалтерия

Таблица данных

Код	Отдел	Уровень конфиденциальности	
AX703	Финансовый	Нет	OK
B789C	Технический	Конфиденциально:проект 1	OK
JFS845	Юридический	Строго конфиденциально:проект1,проект2	X
SF78SD	Отдел кадров	Конфиденциально:проект1:отдел кадров	X

Защита выделенных данных

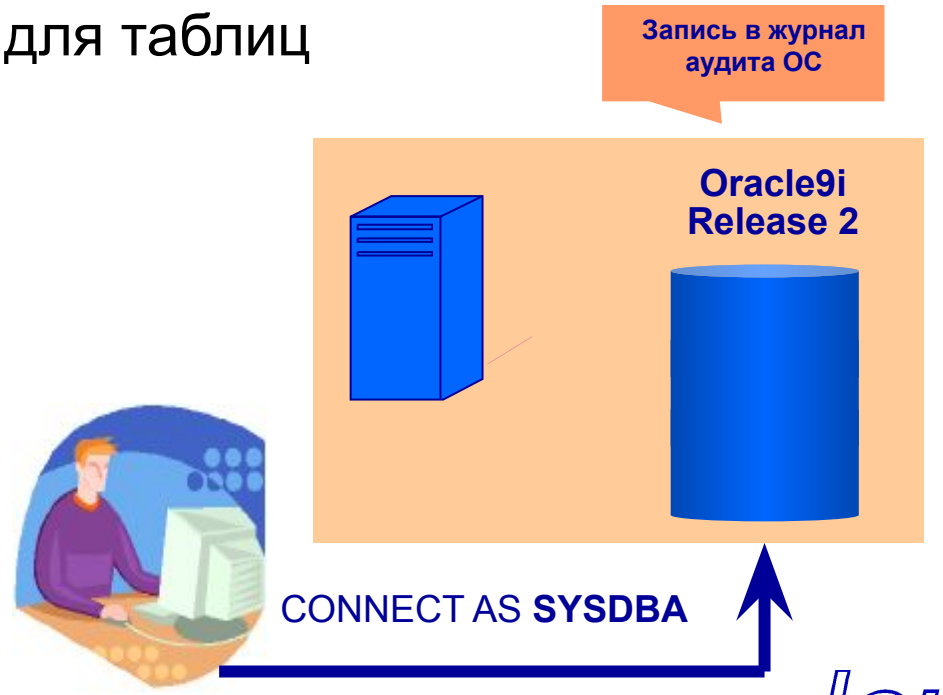
- Предоставляет разработчикам пакет *DBMS_OBFUSCATION_TOOLKIT* для шифрования данных
  - DES, Triple DES (112- and 168-bit keys)
  - MD5 (*криптографическая контрольная сумма*)
- Advanced Encryption Standard (AES):
  - симметричный блочный алгоритм
  - длина блока 128 бит
  - длина ключа 128 (3.4×10^{38}), 192 (6.2×10^{57}) и 256 бит (1.1×10^{77})

Подробнее об AES: http://csrc.nist.gov/encryption/aes/aesfact.html

Расширенный аудит

- Доступ к конкретным объектам схемы
- Контроль использования привилегий
- Контроль использования операторов SQL
- Создание политики аудита для таблиц и представлений
  - предикаты
  - столбец аудита
  - пакет PL/SQL DBMS_FGA
- Аудит административных пользователей

AUDIT_SYS_OPERATIONS = TRUE



Особенности национальной защиты

Были сертифицированы:

- Встроенные средства защиты Oracle Server и Oracle Workgroup Server 7.3.4 по 3 классу защиты от НСД
- Встроенные элементы защиты информации Oracle Server 8.0.3 по классу 1В для АС

Возможные проблемы безопасности

- Использование для получения НСД к данным уязвимостей и ошибок, имеющихся в самом ПО Oracle
- Наличие уязвимостей в настройках ОС, связанных с безопасностью
- Некорректное использование межсетевого экрана, наличие «дыр» в настройках
- Использование паролей по умолчанию, которые «забыли» сменить
- Использование административных ошибок

10 советов по безопасности

1. Установка только необходимых компонентов
2. Блокировка «пользователей по умолчанию» (Default User Accounts)
3. Смена паролей пользователей по умолчанию (Default User Passwords)
4. Защита системного словаря (Data Dictionary)
5. Применение принципа минимизации привилегий

10 советов по безопасности

6. Усиление контроля доступа:
   - ограничение количества пользователей ОС
   - правильная аутенфикация клиентов
7. Ограничение доступа по сети:
   - защита Oracle Server с помощью межсетевого экрана
   - запрет удаленного конфигурирования Oracle Listener
   - шифрование сетевого трафика
   - проверка сетевых настроек ОС
8. Своевременная установка всех обновлений и патчей (Security Patches)
9. Оповещение разработчиков об обнаруженных уязвимостях

Новые компоненты Oracle9i

- Кластеры (Clusters)
- Объединение кэшей (Cache Fusion)
- Сохранение Данных (Data Guard)
- Ретроспективный Запрос (Flashback Query)
- Единая аутенфикация (Single Sign-On)
- Расширенные Средства Безопасности (Advanced Security Option)
- Виртуальная Частная База Данных (Virtual Private Database)
- Детализированный Аудит (Fine-Grained Auditing)
- Интернет-директория (Oracle Internet Directory)

Спасибо за внимание!

Дмитрий Волков
dsvolk@jet.msk.su

Все материалы доступны по адресу

http://dsvolk.msk.ru/oracle/security

Oracle9i – неуязвимый

Unbreakable

Can’t break It. Can’t break.

Что такое неуязвимый и почему

Основные причины остановки системы:

- отказы аппаратных средств
- ошибки в программном обеспечении
- ошибки персонала
- стихийные бедствия
- запланированные перерывы (outage) на обслуживание

Oracle выпустил множество компонент для устранения возможных причин