Основы построения защищенных баз данных

Ваша команда по спасению компьютерной безопасности

17 февраля 2020 г.

Содержание

1 Концепция безопасности БД

Понятие безопасности БД

Угрозы безопасности БД: общие и специфичные

Требования безопасности БД

Защита от несанкционированного доступа

Защита от вывода

Целостность БД

Аудит

Многоуровневая защита

Типы контроля безопасности: потоковый, контроль вывода, контроль доступа

2 Теоретические основы безопасности в СУБД

2.1 Критерии защищенности БД

Критерии оценки надежных компьютерных систем (TCSEC)

Понятие политики безопасности

Совместное применение различных политик безопасности в рамках единой модели

Интерпретация TCSEC для надежных СУБД (TDI)

Оценка надежности СУБД как компоненты вычислительной системы

Монитор ссылок

Применение TCSEC к СУБД непосредственно

Элементы СУБД, к которым применяются TDI: метки, аудит, архитектура системы, спецификация, верификация, проектная документация

Критерии безопасности ГТК

2.2 Модели безопасности в СУБД

Дискреционная (избирательная) и мандатная (полномочная) модели безопасности

Классификация моделей

Аспекты исследования моделей безопасности

Особенности применения моделей безопасности в СУБД

Дискреционные модели: HRU, Take-Grant, Action-Entity, Wood

Мандатные модели: Bell-LaPadula, Biba, Dion, Sea View, Jajodia&Sandhu, Smith&Winslett, решеточная

БД с многоуровневой секретностью (MLS)

Многозначность

3 Механизмы обеспечения целостности СУБД

3.1 Угрозы целостности СУБД

Основные виды и причины возникновения угроз целостности

Способы противодействия

3.2 Метаданные и словарь данных

Назначение словаря данных

Доступ к словарю данных

Состав словаря

Представления словаря

3.3 Понятие транзакции

Фиксация транзакции

Прокрутки вперед и назад

Контрольная точка

Откат

Транзакции как средство изолированности пользователей

Сериализация транзакций

Методы сериализации транзакций

3.4 Блокировки

Режимы блокировок

Правила согласования блокировок

Двухфазный протокол синхронизационных блокировок

Тупиковые ситуации, их распознавание и разрушение

3.5 Ссылочная целостность

Декларативная и процедурная ссылочные целостности

Внешний ключ

Способы поддержания ссылочной целостности

3.6 Правила(триггеры)

Цели использования правил

Способы задания, моменты выполнения

3.7 События

Назначение механизма событий

Сигнализаторы событий

Типы уведомлений о происхождении события

Компоненты механизма событий

4 Механизмы обеспечения конфиденциальности в СУБД

4.1 Классификация угроз конфиденциальности СУБД

Причины, виды, основные методы нарушения конфиденциальности

Типы утечки конфиденциальной информации из СУБД, частичное разглашение

Соотношение защищенности и доступности данных

Получение несанкционированного доступа к конфиденциальной информации путем логических выводов

Методы противодействия. Особенности применения криптографических методов

4.2 Средства идентификации и аутентификации

Общие сведения

Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС

4.3 Средства управления доступом

Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления

Виды привилегий: привилегии безопасности и доступа

Использование ролей и привилегий пользователей

Соотношение прав доступа, определяемых ОС и СУБД

Метки безопасности

Программное зеркалирование

Тиражирование данных

5.4 Системы, обладающие свойством высокой готовности

Описание, назначение, примеры

6 Защита данных в распределенных системах

6.1 Распределенные вычислительные среды

Распределенная обработка информации в среде клиент-сервер

Концепция распределенной вычислительной среды Distributed Computing Environment (DCE)

Распределенные базы данных в сетях ЭВМ

6.2 Угрозы безопасности распределенных СУБД

Угрозы доступности, целостности и конфиденциальности данных

Механизмы противодействия

6.3 Распределенная обработка данных

Понятие распределенной транзакции

Модель обработки транзакций

Мониторы обработки транзакций

Корпоративная среда обработки транзакций

6.4 Протоколы фиксации

Протоколы фиксации

Защищенные протоколы фиксации

Обработка распределенных транзакций в базах данных с многоуровневой секретностью (MLS)

6.5 Тиражирование данных

Обзор средств тиражирования данных

Эффективные алгоритмы тиражирования

Сравнение подходов к тиражированию БД

6.6 Интеграция БД и Internet

Современные тенденции

Обзор существующих технологий

Вопросы безопасности: угрозы и методы противодействия

Перспективы развития

7 Безопасность в статистических БД

7.1 Общие сведения

Определение статистической БД

Классификация статистических БД

Характеристики статистических БД

7.2 Угрозы статистических БД

Статистический вывод

Виды компрометации статистических БД

Методы получения информации из статистических БД

7.3 Защита в статистических БД

Методы защиты от вывода

Статистические фильтры

Статистические функции

Чувствительные статистики

Критерии сравнения методов защиты

8 Распознавание вторжений в БД

8.1 Основные понятия

Определение понятия распознавания вторжений

Цели выявления злоупотреблений

Место процедуры распознавания вторжений в общей системе защиты

8.2 Системы распознавания вторжений

Типы моделей систем распознавания вторжений (ID-систем)

Общая структура ID-систем

Шаблоны классов пользователей

Модели известных атак

8.3 Экспертные ID-системы

Метрики

Статистические модели

Профили

Примеры ID-систем

8.4 Развитие систем распознавания вторжений

Основные тенденции

9 Проектирование безопасности БД

9.1 Основные понятия

Безопасное программное обеспечение

Правила безопасности

9.2 Методология проектирования

Отличия в проектировании безопасных ОС и СУБД

Основные требования к безопасности СУБД

Независимые принципы целостности данных

Модель авторизации в System R

Архитектура безопасной СУБД

Архитектура SeaView и ASD

9.3 Проектирование безопасных БД

Фазы проектирования безопасных БД (по DoD)

Предварительный анализ

Требования и политики безопасности

Концептуальное проектирование

Логическое проектирование

Физическое проектирование

9.4 Формальные верификации и спецификации