Базы данных, лекция 9

@mikhirurg

April 2020

1 Безопасность и защита информации

- Надежность и безопасность БД? СУБД? ИС?

- Что такое безопасная система?
  Что такое безопасная система (Trusted Computer System Evaluation Criteria "The Orange Book"1985).
  Книга о безопасности информационных систем.

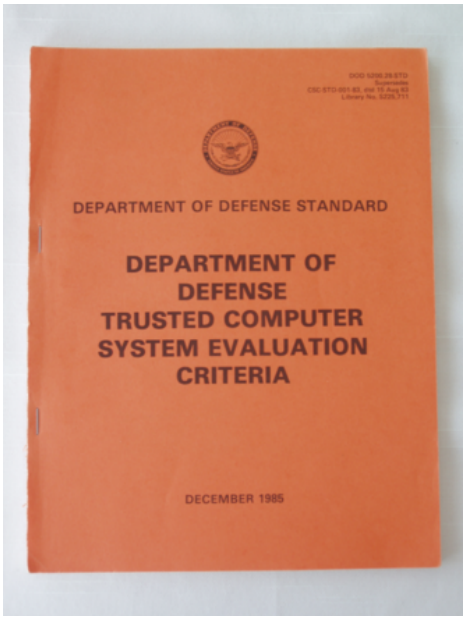

Рис. 1: Trusted Computer System Evaluation Criteria

CRUD — акроним, обозначающий четыре базовые функции, используемые при работе с базами данных: создание (англ. create), чтение (read), модификация (update), удаление (delete).

- Иерархия уровней безопасности:
  - **Класс D** - Система не соответствует другим классам
  - **Класс C** - Есть индентификация, аутентификация, учет событий и дискреционный контроль доступа.
  - **Класс B** - Мандатное управление доступом
  - **Класс A** - Проверенный дизайн

1.1 Системы класса C

- Идентификация, классификация индентификаторов:
  - То, что знает субъект
    Пароль, пин-код, девичья фамилия матери, имя домашнего животного и тд.
  - То, что принадлежит субъекту
    Смарт-карта, мобильный телефон, любой объект, принадлежащий субъекту.
  - То, что является неотъемлимой характеристикой субъекта.
    Биометрия, цифровой почерк.
- Аутентификация, многофакторная аутентификация.
- Авторизация, дискреционный контроль доступа

	Объект1	...	ОбъектM
Субъект1	Read, modify, delete	...	read, change, delegate access
...	...	...	...
СубъектN	Read	...	Read, access to..

Метод определения дискреционногго доступа

- Суперпользователем
- Владельцем
- Делегированием своего доступа (плохо и ненадежно)

1.1.1 Подклассы систем класса C

- **Подкласс C1** Разделение пользователей и данных, контур обеспечения безопасности, дискреционное управление доступом.
  Доступ к объектам имеет изолированная доверенная база.
- **Подкласс C2** Доступ через процедуру авторизации, журнал контроля доступа к системе, изоляция ресурсов.
  Выделяя память, мы должны быть уверены, что её нельзя проанализировать и получить доступ к информации, обрабатываемой другим процессом ранее.

1.2 Системы Класса B

Системы мандатного управления доступом.
То есть для того, что бы получивший доступ субъект не мог нарушить конфеденциальность доступность данных используется мандатный доступ с помощью меток доступа.
'Жесткое' Правило:

- Чтение своего уровня и ниже
- Запись на свой уровень и уровень выше

1.2.1 Подклассы класса B

- **Подкласс B1** - Мандатное управление доступа к выбранным субъектам и объектам, изоляция процессов.
- **Подкласс B2** - Структурированная защита - применение мандатного управления ко всем объектами субъектам, отдельный защищенный способ первичной индентификации и аутентификации, модульная структура контура безопасности.
- **Подкласс B3** Домены безопасности - выделенный администратор системы безопасности, мониторинг обращений

1.3 Системы класса A

- Формализированные процедуры проектирования
- Формализированные процедуры упревления
- Формализированные процедуры распространения

1.4 Ролевая модель доступа

- Преимущества
  - Сокращение операции назначения и проверки прав доступа
  - Централизация управления
- Типовые роли
  - Администратор СУБД
  - Админ БД
  - Привелегированный пользователь
  - Обычный пользователь

1.5 Аудит безопасности

Протоколирование
Записывать каждую попытку аутентификации не очень удобно, так как это потредует большого расхоба памяти + обрабатывать огромные логи долго.
Выборочное протоколирование - записываем каждую n-ую попытку входа.
Адаптивное протоколирование - запись попыток в записимости от некоторого условия.

1.6 Шифрование баз данных

- Прозрачное шифрование
- Column-level encryption - Шифрование на уровне столбцов. Удобно разделять доступ к разным столбцам.
- Шифрование файловой системы.
  удобно исспользовать в распределённых системах
- Шифрование на уровне приложений
  База данных не занимается шифрованием, это делают сами приложения.
  Минус: невозможно адекватное индексирование по шифрованным данным
- Hashing - Хэширование - паролю пользователя сопоставляется результат некоторой хеш-функции.

Угроза действий привелегированных пользователей. Решение проблемы:

- Резервное копирование