ЛАБОРАТОРНАЯ РАБОТА №3
«ПАРОЛЬНАЯ ЗАЩИТА»
Вариант 5

Плотников Антон, А3401

Санкт-Петербург, 2017

1. Вопросы

1.1. Что дает присвоение каждому пользователю уникального идентификатора?

Это позволяет вводить различный уровень прав доступа пользователей к информации и позволяет возможность полного учета всех входов пользователей в систему в журнале аудита.

1.2. Чем определяется стойкость к взлому подсистемы идентификации и аутентификации?

Видом идентификатора, способом аутентификации и тем как организован обмен данными для аутентификации.

1.3. Чем определяется сложность подбора пароля? Как производится количественная оценка стойкости парольных систем?

Количественная оценка может быть выполнена по формуле:

$$P = \frac{V \times T}{S} = \frac{V \times T}{A^L},$$

где $S = A^L$ — число возможных паролей длины L, которые можно составить из алфавита мощности A; V — скорость перебора паролей; T — максимальный срок действия паролей.

1.4. Сравните сложность подбора представленных паролей: *18_JcT*a* (символы верхнего и нижнего регистров, цифры, специальные символы) и *Jf1UGwxRd* (символы верхнего и нижнего регистров, цифры).

Положим скорость перебора паролей разной, тогда разницу в формулу включает только мощность алфавита и длина пароля, причем длина пароля является показателем степени и вносит больший вклад. Тогда сложность перебора пароля длины 9 выше не смотря на менее мощный алфавит.

1.5. Какие недостатки есть у такого метода противодействия подбору паролей, как ограничение числа попыток ввода пароля? Чем его можно заменить?

Недостаток в том, что вероятность подбора пароля за ограниченное число попыток все же существует, а так же существует вероятность частой блокировки ”забывчивых” пользователей. В качестве решения проблемы можно использовать трехфакторную аутентификацию.

1.6. Как изменится стойкость к взлому подсистемы парольной аутентификации при увеличении характеристик A, L, V, T? При их уменьшении?

Изменение параметров V и T вносят линейный вклад в формулу расчета стойкости (при уменьшении параметров увеличивается стойкость). Изменение параметров A и L изменяют стойкость по степенному и показательному закону соответственно (при увеличении параметров увеличивается стойкость).

1.7. В каком виде пароли могут храниться в БД учетных записей? Опишите недостатки этих видов хранения.

Пароли в базе данных можно хранить в шифрованном или хешированном виде.

Для шифрованного хранения необходимо обеспечить безопасный обмен ключом шифрования. В случае получения злоумышленником ключа шифрования у него будет возможность получить пароли пользователей в открытом виде.

Недостатком хеширования является невозможность восстановления пароля пользователя.

1.8. Какой метод может применяться для сокрытия паролей в БД от администратора. Как этот метод может быть усилен для предотвращения подбора паролей?

Хеширование паролей на клиентской стороне. Автоматическая генерация паролей, принудительная смена ”пароля по умолчанию”.

1.9. Приведите примеры технических устройств, с помощью которых может решаться задача идентификации и аутентификации пользователя?

- USB ключи
- Пластиковые карты
- Идентификаторы iButton
- Бесконтактные радиочастотные карты proximity

1.10. Какие биометрические характеристики применяются для аутентификации? В чем преимущества этого способа аутентификации?

- Отпечатки пальцев
- Геометрическая форма рук
- Особенности голоса
- Рисунок радужной оболочки глаза
- Форма и размеры лица

Преимуществом является то, что зачастую очень сложно подделать биометрические параметры, и для аутентификации необходимо иметь часть тела пользователя.

2. Задачи

Задача 1. Определить время перебора всех паролей с параметрами.

Алфавит состоит из $A = 59$ символов. Длина пароля составляет $L = 5$ символов. Скорость перебора $V = 200$ паролей в секунду. После каждого из $m = 0$ неправильно введенных паролей идет пауза в $v = 0$ секунд.

Решение.

$$t = \frac{A^L}{V} = \frac{59^5}{200} \text{ сек.} = 3574621.495 \text{ сек.} \approx 41 \text{ дней}$$

Задача 2. Определить минимальную длину пароля, алфавит которого состоит из $A = 59$ символов, время перебора которого было бы не меньше $t = 50$ лет. Скорость перебора $V = 200$ паролей в секунду.

Решение.

$$L = \log_A(t \times V) = log_{59}(50 \times 365 \times 24 \times 60 \times 60 \times 200) \approx 6.5 < 7$$

Задача 3. Определить количество символов алфавита, пароль которого состоит из $L = 9$ символов, время перебора которого было бы не меньше $t = 50$ лет. Скорость перебора $V = 200$ паролей в секунду.

Решение.

$$A = \sqrt[L]{t \times V} = \sqrt[9]{50 \times 365 \times 24 \times 60 \times 60 \times 200} \approx 18.95 < 19$$