Парольные системы идентификации и аутентификации пользователей

Совокупность идентификатора и пароля пользователя - основные составляющие его ***учетной записи***. *База данных пользователей* парольной системы содержит учетные записи всех пользователей КС, при этом сами пароли шифруются администратором сети, обычно с использованием хэш-функций.

**Парольные системы являются зачастую «передним краем обороны» всей системы безопасности**. Отдельные ее элементы могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику (в том числе и база данных учетных записей пользователей). В связи с этим, парольные системы становятся одним из наиболее привлекательных для злоумышленника объектов атаки. Основными типами угроз безопасности парольных систем являются следующие:

* Перебор паролей в интерактивном режиме.
* Подсмотр пароля.
* Преднамеренная передача пароля его владельцем другому лицу.
* Кража базы данных учетных записей с дальнейшим ее анализом,
* подбором пароля.
* Перехват вводимого пароля путем внедрения в КС программных
* закладок (клавиатурных шпионов); перехват пароля, передаваемого
* по сети.
* Социальная инженерия.

Многие недостатки парольных систем связаны с наличием человеческого фактора, который проявляется в том, что пользователь зачастую стремится выбрать пароль, который легко запомнить (а значит и подобрать), записать куда-нибудь свой сложный пароль. Легальный пользователь способен ввести пароль так, что его могут увидеть посторонние, передать пароль другому лицу намеренно или под влиянием заблуждения.

Для уменьшения деструктивного влияния человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

*Задание минимальной длины пароля* для затруднения подбора пароля злоумышленником «в лоб» и подсмотра.

*Использование в пароле различных групп символов* для усложнения подбора злоумышленником пароля.

*Проверка и отбраковка пароля по словарю* для затруднения подбора пароля злоумышленником с использованием словарей.

*Установление максимального срока действия пароля* для затруднения подбора пароля злоумышленником, в том числе и в режиме «off-line» при взломе предварительно похищенной базы данных учетных записей пользователей.

*Применение эвристического алгоритма, бракующего «плохие»**пароли* для усложнения подбора пароля злоумышленником «по словарю» или с использованием эвристического алгоритма.

*Ограничение числа попыток ввода пароля* для предотвращения интерактивного подбора пароля злоумышленником.

*Использование задержки при вводе неправильного пароля* для предотвращения интерактивного подбора пароля злоумышленником.

*Поддержка режима принудительной смены пароля пользователя* для эффективности реализации требования, ограничивающего максимальный срок действия пароля.

*Запрет на выбор пароля самим пользователем и автоматическая генерация паролей* для затруднения использования злоумышленником эвристического алгоритма подбора паролей.

Количественная оценка стойкости парольных системможет быть выполнена с помощью рассматриваемого ниже подхода.

Пусть *A*– мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля). Например, если при составлении пароля могут быть использованы только малые английские буквы, то *A*=26.

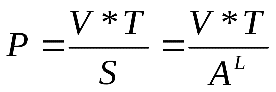
*L*– длина пароля.

https://studfile.net/html/2706/212/html_cbOWVPda0Y.hx7q/img-ETlY_K.png - число всевозможных паролей длины *L*, которые можно составить из символов алфавита *A*. *S*также называют *пространством атаки*.

*V*– скорость перебора паролей злоумышленником.

*T*– максимальный срок действия пароля.

Тогда, вероятность *P* подбора пароля злоумышленником в течении срока его действия *Т* определяется по следующей формуле.



Эту формулу можно обратить для решения следующей задачи:

*Задача*. Определить минимальную мощность алфавита паролей *A* и минимальную длину паролей *L*, обеспечивающих вероятность подбора пароля злоумышленником не более заданной *P*, при скорости подбора паролей *V*, максимальном сроке действия пароля *T*.

Данная задача имеет неоднозначное решение. При исходных данных ***V,T,P*** однозначно можно определить лишь нижнюю границу *S\**числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле:

|  |  |
| --- | --- |
| https://studfile.net/html/2706/212/html_cbOWVPda0Y.hx7q/img-Z0BN6P.png | (3.1) |

где https://studfile.net/html/2706/212/html_cbOWVPda0Y.hx7q/img-7awV9E.png- целая часть числа, взятая с округлением вверх.

После нахождения нижней границы *S\**необходимо выбрать такие *A* и *L*, чтобы выполнялось неравенство (3.2):

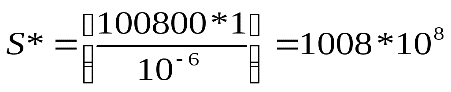
|  |  |
| --- | --- |
| https://studfile.net/html/2706/212/html_cbOWVPda0Y.hx7q/img-TKQSqy.png | (3.2) |

При выборе *S*, удовлетворяющего неравенству (3.2), вероятность подбора пароля злоумышленником (при заданных *V* и *T*) будет меньше или равна *P.*

При вычислениях по формулам (3.1) и (3.2), величины должны быть приведены к одной размерности.

*Пример 3.1*

Пусть задано: *P*=10-6,*T*=7 дней, *V*=10 паролей / минуту = 10\*60\*24\*7=100800 паролей в неделю.

Тогда, .

Условию https://studfile.net/html/2706/212/html_cbOWVPda0Y.hx7q/img-FAy6Y4.pngудовлетворяют, например, такие пары величин *A* и *L*, как *A*=26, *L*=8 (пароли состоят из 8 малых символов английского алфавита), *A*=36, *L*=6 (пароли состоят из 6 символов, среди которых могут быть малые латинские буквы и цифры).