

«КОЛИЧЕСТВЕННАЯ ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ»

Цель работы – реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Теоретический материал

Подсистемы идентификации и аутентификации пользователя играют очень важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае, информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя является, как правило, передним краем обороны СЗИ. В связи с этим, модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель злоумышленника в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя являются наиболее простыми методами аутентификации и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю

1. Минимальная длина пароля должна быть не менее 6 символов.
2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы '(', ')', '#', и т.д.).
3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации.

1. Администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, он должен быть сменен.
2. В подсистеме парольной аутентификации должно быть установлено ограничение числа попыток ввода пароля (как правило, не более 3).
3. В подсистеме парольной аутентификации должна быть установлена временная задержка при вводе неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы - автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации, единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то $A=26$).

L – длина пароля.

$S = A^L$ - число всевозможных паролей длины L , которые можно составить из символов алфавита A .

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

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

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

Эту формулу можно использовать в обратную сторону для решения следующей задачи:

ЗАДАЧА. Определить минимальные мощность алфавита паролей A и 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

$$S^* = \left[\frac{V * T}{P} \right] \quad (1)$$

где $[]$ - целая часть числа, взятая с округлением вверх.

После нахождения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось неравенство (2).

$$S^* \leq S = A^L \quad (2)$$

При выборе S , удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P .

Необходимо отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример

Исходные данные – $P=10^{-6}$, $T=7$ дней = 1 неделя, $V=10$ паролей / минуту = $10*60*24*7=100800$ паролей в неделю.

$$\text{Тогда, } S^* = \left[\frac{10800 * 1}{10^{-6}} \right] = 108 * 10^8.$$

Условию $S^* \leq A^L$ удовлетворяют, например, такие комбинации A и L , как $A=26$, $L=8$ (пароль состоит из 8 малых символов английского алфавита),

$A=36$, $L=6$ (пароль состоит из 6 символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Задание на лабораторную работу

1. В таблице 1 найти для вашего варианта значения характеристик P, V, T .
2. Вычислить по формуле (1) нижнюю границу S^* для заданных P, V, T .
3. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L , при котором выполняется условие (2).
4. Оформить отчет по лабораторной работе согласно примеру, приведенному на последней странице.

Таблица 1

Вариант	P	V	T
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Контрольные вопросы.

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течении срока его действия?
5. Выбором каким параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Пример оформления отчета по лабораторной работе

ЛАБОРАТОРНАЯ РАБОТА №

НАЗВАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

ВЫПОЛНИЛ: ст. гр. ФИО

ВАРИАНТ № ...

ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

$P=...$

$V=...$

$T=...$

$S^*=$ (привести вычисления) =

В качестве алфавита символов, используемых при генерации пароля, был выбран следующий набор _____. Мощность данного набора $A=$ _____.

При минимальном значении $L=...$ выполняется условие $S^* \leq S = A^L$.

Для реализации генератора паролей были выбраны значения $A=...$ и $L=...$, при которых заведомо выполняется условие $S^* \leq A^L$.