МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ ПАРОЛЬНЫХ СИСТЕМ

Салита Д.С., Удовик А.А.
Алтайский государственный университет, г. Барнаул
d.s.salita@gmail.com

Аннотация. Рассмотрены методики оценки стойкости паролей, которые позволяют с помощью набора определённых критериев количественно оценить надёжность пароля к взлому. Показано, как мощность алфавита пароля (наличие цифр, символы в верхнем и нижнем регистрах и специальные символы) и длина влияют на его стойкость к полному перебору. Предложены рекомендации для увеличения надёжности применяемых паролей.

Ключевые слова: информационная энтропия, пароль, сложность пароля.

В настоящее время на практике используется большое количество различных способов аутентификации пользователей. Однако из всего разнообразия методов можно выделить парольные системы аутентификации, которые являются самыми распространёнными. Применение паролей в информационных системах позволяет организовать разграничение доступа к ресурсам локальной или корпоративной сети. Кроме того, пароль можно также использовать для установления шифрованного канала между двумя собеседниками для передачи данных по сети [1]. Однако из-за своей распространённости парольные системы в большей степени подвержены атакам злоумышленников.

Существует две основные проблемы, с которыми аутентификационные системы на основе паролей встречаются чаще всего. Во-первых, это человеческий фактор. Для полноценной защиты конфиденциальной информации используются длинные и сложные пароли, состоящие из случайного сочетания цифр, символов и специальных знаков [2,4]. Такие пароли считаются надёжными, но пользователи не всегда способны их запомнить и использовать в корпоративных сетях или в личном пользовании.

Во-вторых, техническое несовершенство реализации парольных систем. Наиболее распространённой ошибкой является хранение паролей пользователей в открытом виде. В случае успешной проведённой атаки на такой сервис, злоумышленник может получить доступ к базе данных с логинами и паролями пользователей. Применение хэширования позволяет обезопасить данные пользователей даже в случае завладения ими третьей стороной.

Для снижения деструктивного влияния человеческого фактора необходимо определить минимально допустимые требования к используемым паролям. Существует несколько способов для количественной оценки надёжности пароля. Одним из таких методов является энтропия [3]. Это мера неопределенности, которая измеряется в битах. Например, мера неопределенности, состоящая из 1-го бита, соответствует двум паролям, а пароль с энтропией в 32 бита потребует 2^{32} (4 294 967 296) попыток, чтобы использовать все возможности во время перебора. В общем случае информационная энтропия случайного пароля E определяется по формуле:

$$E = \log_2 M^N \quad (1)$$

где M – мощность алфавита паролей, N – длина пароля.

В таблице 1 приведены значения энтропии для некоторых комбинаций паролей, состоящих из цифр и латинского алфавита [5]. Можно заметить, что разные по длине и мощности алфавита пароли имеют схожее значение энтропии. Например, пароль состоящий из 10 цифр эквивалентен паролю, содержащему 7 букв латинского алфавита без учёта регистра.

Таблица 1. Значения энтропии для некоторых длин паролей.

Количество символов в пароле	Цифры	Латинские буквы без учета регистра	Латинские буквы с учетом регистра	Цифры и латинские буквы без учета регистра	Цифры и латинские буквы с учетом регистра
6	19.9	28.2	34.2	31.0	35.7
7	23.3	**32.9**	39.9	36.2	41.7
8	26.6	37.6	45.6	41.4	47.6
10	**33.2**	47.0	57.0	51.7	59.5
11	36.5	51.7	62.7	56.9	65.5
12	39.9	56.4	68.4	62.0	71.5

Метрика на основе энтропии используется различными методами для расчета коэффициента надежности пароля. Одним из таких методов является Password Strength Tester [6]. В зависимости от полученного значения энтропии, паролю присваивается соответствующая характеристика его стойкости (рис. 1).

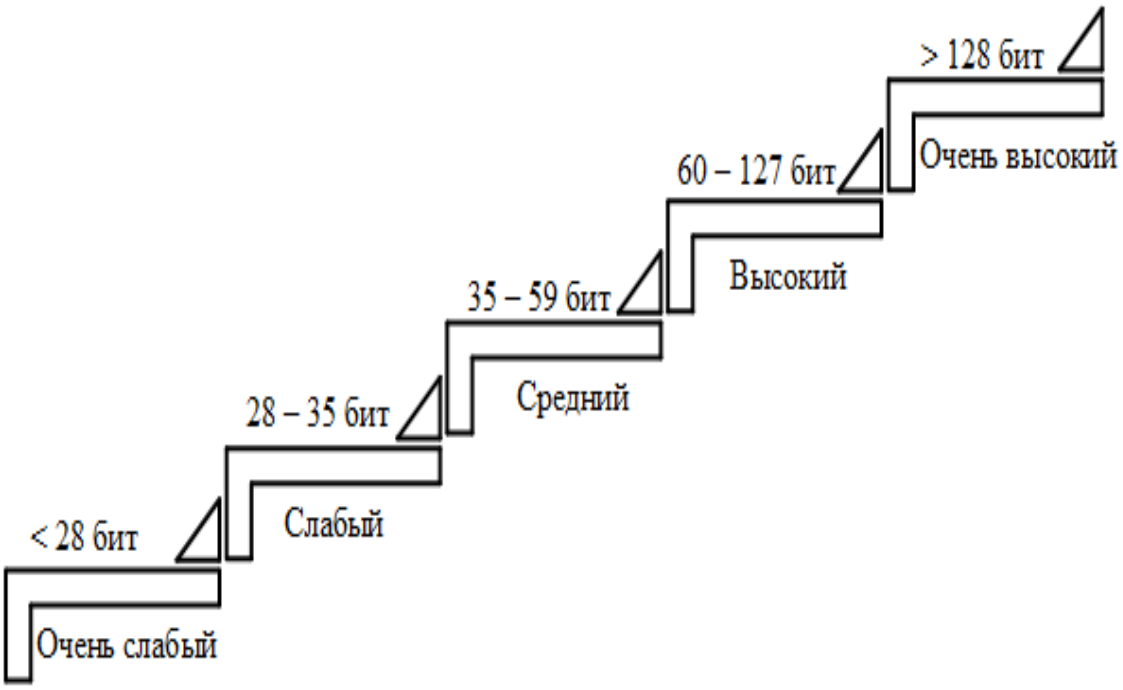

Рисунок 1. Зависимость уровня стойкости пароля от значения энтропии.

Описание уровней стойкости:

–Очень слабый – разрешимо защищать только не ценную информацию;

–Слабый – данный тип паролей способен предотвратить атаку начинающих злоумышленников;

–Средний – пароли с уровнем «Средний» используются в корпоративных сетях;

–Высокий – пароль со статусом «Высокая сложность» используются для защиты конфиденциальной или финансовой информации;

–Сверхнадежный – пароль обладает очень большой стойкостью к подбору.

Качественно другая методика, позволяющая исключить коллизии, используется в анализаторе надёжности паролей Password Strength Meter [7]. В процессе работы данного метода анализируется количество используемых символов, а именно количество английских символов в верхнем и нижнем регистре, цифр и специальных символов. В зависимости от их количества выставляются определенные коэффициенты.

Алгоритм расчета коэффициента надежности пароля с помощью Password Strength Meter состоит из следующих шагов:

1. Параметр надежности пароля приравнивается к нулю;
2. Если длина пароля не соответствует установленному минимальному порогу, то алгоритм прекращается, если пароль равен или больше минимального порога, то вес пароля увеличивается на величину 4*len, где len – длина пароля. Минимальный порог равен 4 символа в пароле;
3. На следующем шаге проводится сканирование пароля на наличие подряд идущих одинаковых символов, например, используя данный алгоритм к паролю «aaabbvad», результатом будет следующий пароль «abvad». После алгоритма сжатия пароля, происходит уменьшение веса пароля на величину *len-len_compress*, где *len* – исходная длина пароля, а *len_compress* – длина пароля после сжатия. Процедура сжатия пароля происходит до тех пор, пока не удалятся все одинаковые подряд идущие символы. Важно, сжатие каждый раз производиться на проверяемом пароле, а не на строках, полученных в результате предыдущих сжатий;
4. После сжатия пароля происходит увеличение веса пароля по определенным параметрам (рис. 2):
   - Наличие цифр;
   - Наличие специальных символов;
   - Наличие символов в верхнем и нижнем регистрах;
   - Сочетание цифр и символов;
   - Сочетание цифр и специальных символов;
   - Сочетание символов и специальных символов;

Также возможно и уменьшение веса пароля по следующим параметрам (рис. 1):

- Пароль, состоящий только из цифр;
- Пароль, состоящий только из букв.

На следующем шаге работы алгоритма происходит нормализация: если вес пароля меньше 0, то установить его равным 0. Если больше 100, то установить равным 100;

Считается, что если стойкость анализируемого пароля меньше 34-х, то данный пароль является не надежным, и может использоваться только для защиты не конфиденциальной информации. Если вес пароля от 34 до 67, то пароль относится к категории «Хороший», а если более 67, то пароль считается надежным.

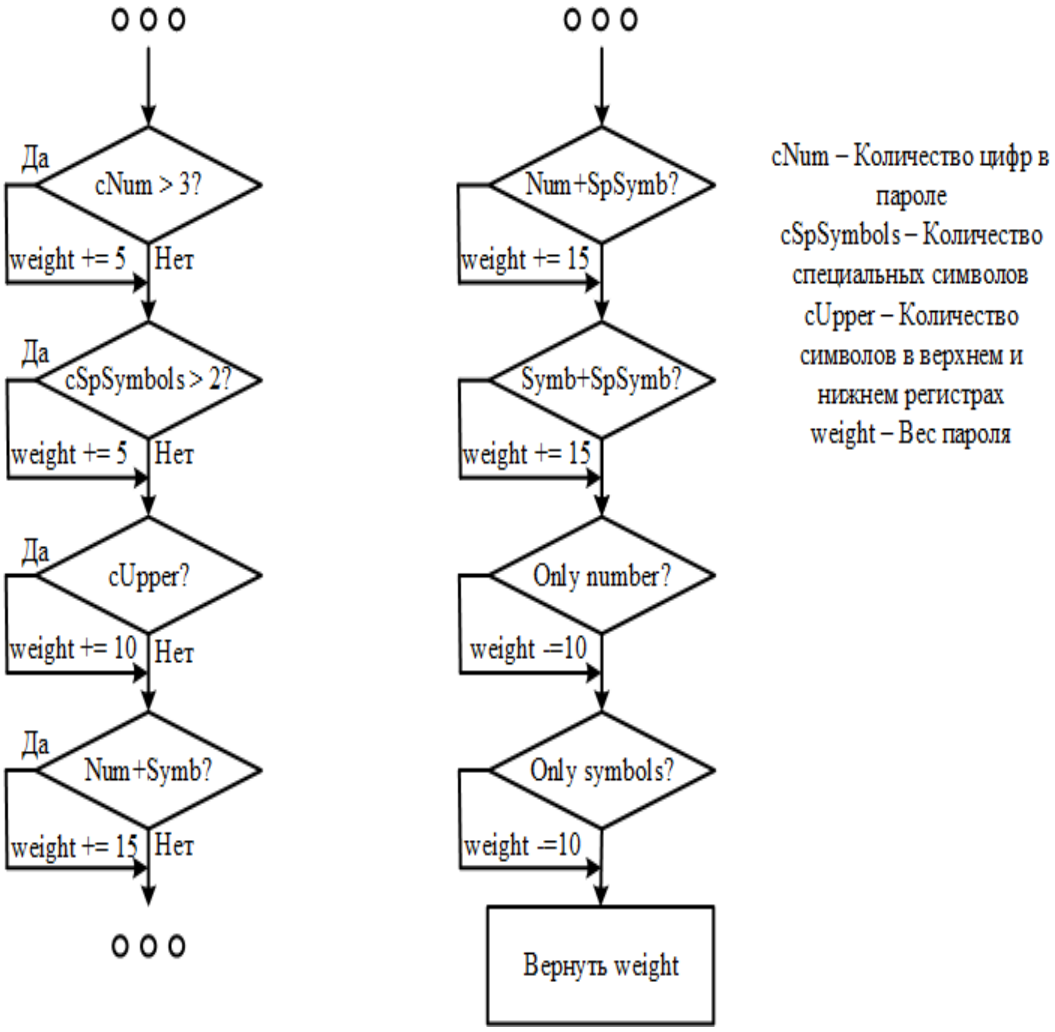

Рисунок 2 - Алгоритм увеличение и уменьшение веса пароля.

Рассмотренные метрики оценки стойкости паролей позволяют по определенному набору признаков дать количественную оценку стойкости пароля ко взлому. В зависимости от области применения критерии оценивания надежности могут меняться, однако минимальный набор требований к мощности алфавита и длине паролей в большинстве случаев совпадает: наличие цифр, символов в верхнем и нижнем регистрах, специальные символы, а длина пароля должна быть не менее 6 символов.

Библиографический список

1. Бирюков Андрей Александрович, Информационная безопасность / Бирюков Андрей Александрович, Информационная безопасность, защита и нападение – ДМК-Пресс 2017 – 434 с.
2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации // Руководящий документ ФСТЭК России 30 марта 1992
3. Гуфан К.Ю., Новосядлый В.А., Эдель Д.А. Оценка стойкости парольных фраз к методам подбора // Открытое образование. 2011. №2. 127-130 с.
4. Заркумова Р.Н. Исследование количественных характеристик системы парольной защиты информации // Сборник научных трудов НГТУ. 2010. № 2(60). С.83-88.

5. Марков Г.А. Метрики стойкости парольной защиты // Молодежный научно-технический вестник. – 2013.
6. Интернет ресурс «Rumkin.com» [Электронный ресурс] Режим доступа: http://rumkin.com/tools/password/passchk.php
7. Интернет ресурс «Visual Password Strength Indicator Plugin For jQuery» [Электронный ресурс] Режим доступа: https://www.jqueryscript.net/form/Visual-Password-Strength-Indicator-Plugin-For-jQuery-Passtrength-js.html

PASSWORD SYSTEM RELIABILITY ASSESSMENT METHODS

Salita D.S., Udovik A.A.
Altai State University, Barnaul
e-mail: d.s.salita@gmail.com

Abstract. Methods of password resistance assessment are considered, which make it possible to quantify password reliability to hacking using a set of certain criteria. It is shown how the power of the password alphabet (the presence of numbers, characters in the upper and lower registers and special characters) and the length affect its resistance to complete search. Recommendations are offered to increase the reliability of the passwords used.

Keywords: information entropy, password, password difficulty.