Научная статья
Original article

Анализ надежности паролей для защиты данных

Назарова А.Д.
Уральский государственный экономический университет, Екатеринбург, Россия
Автор-корреспондент: nazarova-aleks2002@mail.ru

Аннотация: В этой статье рассмотрены рекомендации создания безопасного пароля для защиты личных данных. Проведен анализ с помощью HOW SECURE IS MY PASS-WORD для поиска ключевых показателей при подборе паролей.

Ключевые слова: пароль, надежность пароля, защита личных данных.

Для цитирования: Назарова А.Д. Анализ надежности паролей для защиты данных. Умная цифровая экономика. 2022. Т.2, №4, с. 41-46

Password Strength Analysis for Data Protection

Nazarova A.D.
Ural State University of Economics, Ekaterinburg, Russia

**Corresponding author: nazarova- aleks2002@mail.ru*

Abstract: The article presents an analysis of the ways, conditions and means of using IT - technologies in the improvement of automotive transport systems. Arguments are given proving that in modern conditions it becomes technically possible to implement digital transport management on currently functioning roads.

Keywords: digitalization of roads, transport accessibility, mobility.

For citation: Nazarova A.D. Password Strength Analysis for Data Protection. Smart Digital Economy. 2022. T.2, №4, pp. 41-46.

Интернет стал неотъемлемой частью жизни каждого человека. В современном мире происходит стремительное развитие информационных технологий: каждый день увеличивается количество пользователей в социальных сетях, Интернет-ресурсах, мобильных приложений банков и т.д. Этот фактор повлиял на то, что стало больше сайтов, на которых нужна авторизация для защиты от злоумышленников.

Любая регистрация предполагает создание логина и пароля. Логин может быть любой индивидуальной последовательностью символов. А в качестве пароля необходимо подобрать какой-то набор букв, который является надежным.

Одно из ранних упоминаний чего-то похожего на пароль возникло ещё задолго до появления компьютеров в 6-7 веке в библейской Книге Судей, но оптимизация защиты секретных и не обязательно секретных данных именно на ПК началась еще с 90-х годов, когда американский ученый по имени Фернандо Корбато создал операционную систему, где был

представлен вход по паролю. Одной из главных задач в ходе ее создания было распределение ценнейшего ресурса — времени, в течение которого люди могли работать с системой. После ввода пароля человек мог работать в течение четырех часов, за которые нужно было успеть выполнить максимум задач [2]. «Система разделения времени» (CTSS) − так называлось в то время данное открытие. В то время изобретение стало сенсацией в мире информационных технологий, что значительно укорило процесс работы за персональным компьютером. Каждый пользователь мог войти по паролю и получить доступ к личным данным.

Пароль – это простая форма реализации информационной безопасности; набор знаков, состоящий из букв, цифр и других символов, и предназначенный для подтверждения личности или полномочий.

Целью нашего исследования является выделение основных рекомендаций по созданию надежного секретного кода с помощью сервиса оценки надежности паролей.

Суть сайта для проверки паролей заключается в оценке надежности любого подбора символов и проверки безопасности, посмотрев сколько времени понадобится чтобы злоумышленник смог вас взломать. Надежность пароля зависит от длины, сложности и непредсказуемости.

Использование надежных паролей снижает общий риск нарушения безопасности, но надежные пароли не заменяют необходимость в других эффективных мерах безопасности. Эффективность пароля заданной сложности во многом определяется дизайном и реализацией программного обеспечения системы аутентификации, в частности тем, как часто злоумышленник может проверять угадываемый пароль и насколько надежно хранится, и передается информация о паролях пользователей.

Область применения паролей затрагивает все сферы человеческой жизни, кто имеет или ответственен за доступ к конфиденциальной информации всех уровней (или любая форма доступа, которая поддерживает или требует пароля) на любой системе [3].

Как выбрать безопасный пароль?

Вариантов может быть два: длинный пароль сложный в запоминании, но надежный, а также короткий пароль легкий в запоминании, но небезопасный для защиты конфидициальных данных. Существуют несколько правил создания надежного пароля, такие как использование множества различных символов: строчные буквы, заглавные буквы, а также специальные символы: №;%:?*()_+=-. Для надежного пароля нужно использовать комбинации из символов различной категории. Приведем пример с помощью сервиса генератора паролей HOW SECURE IS MY PASS-WORD для проверки теории.

Придумаем пароль только из цифр длиною 11 символов. Как показано на рисунке 1, пароль будет взломан за 2 секунды.

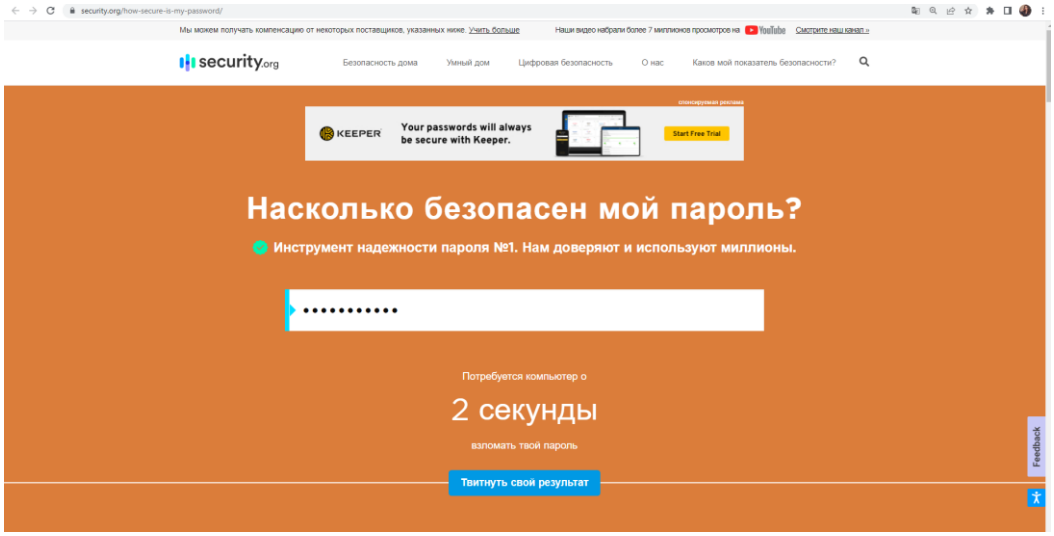

Рисунок 1. Пример пароля из 11 символов

Следующим примером будет пароль из цифр, строчных и заглавных букв длиною в 9 символов будет взламываться за 2 недели (рисунок 2).

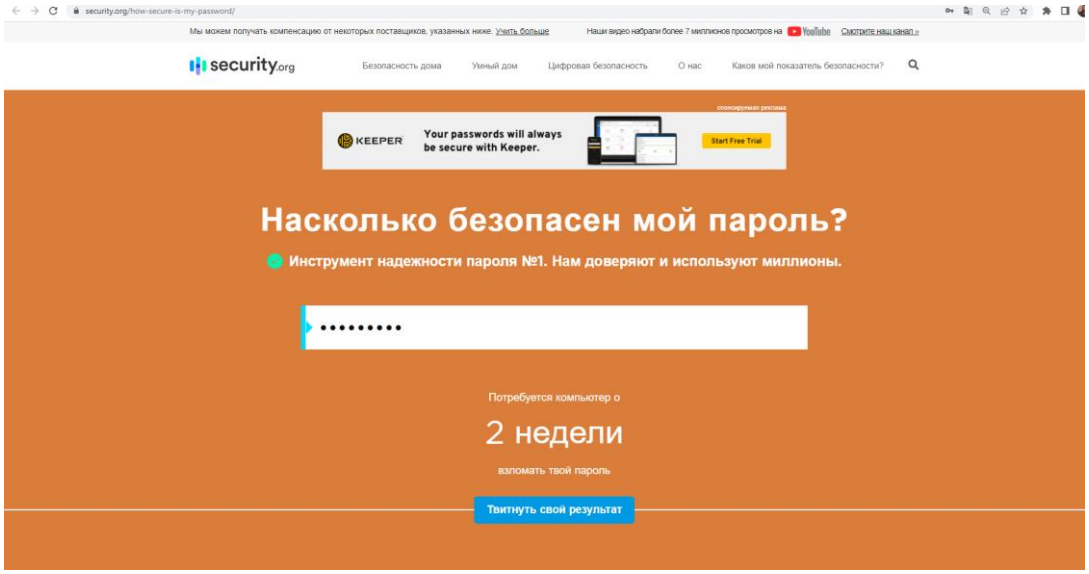

Рисунок 2. Пример пароля из 9 символов

Поскольку в пароле могут использоваться любые символы, было принято решение проклассифицировать и разделить возможные пароли по нескольким признакам.

Пароль, состоящий из цифр. Итак, в данном тестировании прослеживается зависимость между количеством символов в пароле и потраченным временем на взлом. Делаем вывод, что от самих символов на данном сайте надежность не зависит (рисунок 3).

Характеристика	Примеры паролей	Количество символов в пароле	Время
Числовая запись	23445556...	17	6 часов
	11111...	18	41 минута
	333...	19	7 лет
	777...	16	2 дня

Рисунок 3. Пароль, состоящий из цифр

Пароль из строчных латинских букв. Таким образом, второй опыт показал, что компетентность зависит от самих символов и их комбинаций. Приемлемое количество символов в пароле 11, время – 1 неделя (рисунок 4).

Характеристика	Примеры паролей	Количество символов в пароле	Время
Запись латинских строчных букв и чисел	ssss...	11	1 неделя
	5dfj555...	12	23 года
	2222aaaaa...	10	4 дня
	aaa555aaa...	11	6 месяцев

Рисунок 3. Пароль из строчных латинских букв

Пароль из заглавных латинских букв. В данном пункте было проверено значение различных букв при одинаковом количестве символов и разницу результатов при одинаковых комбинациях, но разной длины. Результат оказался таким же, как и предыдущих опытах – прямая зависимость (рисунок 5).

Характеристика	Примеры паролей	Количество символов в пароле	Время
Запись заглавных латинских букв	DJHC...	12	3 недели
	DDD...	15	29 лет
	SSS...	11	1 неделя
	GHY...	17	30 млн.лет

Рисунок 4. Пароль из заглавных латинских букв

Пароль, состоящий из строчных и заглавных букв латинского алфавита. Для начала мы проверили чередованием, есть ли разница между разными положениями символов или учетом регистра и зависит ли надежность пароля от количества тех и других или от самих символов. Результат не изменился (рисунок 6).

Характеристика	Примеры паролей	Количество символов в пароле	Время
Запись строчных и заглавных латинских букв	SSSdfg...	11	5 лет
	SdFdGs...	12	3 сотни лет
	ddsFF...	13	1 миллион лет
	dEdS...	7	1 минута

Рисунок 6. Пароль, состоящий из строчных и заглавных букв латинского алфавита

Пароль, состоящий из цифр и строчных/заглавных букв, а также и из цифр, строчных и заглавных латинских букв. Следующие три испытания проходили отдельно, но исход оказался одинаковым: на изменение надежности не повлияли ни комбинации букв и цифр, ни различие (разнообразие) символов, ни соотношение количества букв к цифрам, а только их суммарное количество. В третьем тестировании тот же самый вывод, но единственная разница заключается во времени, точнее в том, что, при одинаковом количестве символов по сравнению с предыдущими двумя опытами, требуется большее время, нужное на взлом пароля. При появлении еще одного типа символов, повысился уровень сложности пароля, что и отразилось на его надежности. Все полученные результаты можно увидеть на рисунке 7.

Характеристика	Примеры паролей	Количество символов в пароле	Время
Числовая запись	23445556...	17	6 часов
	11111...	18	41 минута
	333...	19	7 лет
	777...	16	2 дня
Запись латинских строчных букв и чисел	ssss...	11	1 неделя
	5dfj555...	12	23 года
	2222aaaaa...	10	4 дня
	aaa555aaa...	11	6 месяцев
Запись заглавных латинских букв	DJHC...	12	3 недели
	DDD...	15	29 лет
	SSS...	11	1 неделя
	GHY...	17	30 млн.лет
Запись строчных и заглавных латинских букв	SSSdfg...	11	5 лет
	SdFdGs...	12	3 сотни лет
	ddsFF...	13	1 миллион лет
	dEdS...	7	1 минута
Запись цифр и латинских строчных букв	111dd...	9	2 часа
	234dfda2..	11	1 год
	shd3...	12	3 года
	234dh..	14	1 миллион лет
Запись цифр и латинских заглавных букв	111DD...	11	4 года
	23FF...	10	2 года
	1B4A...	12	5 лет
	2F364F...	14	9 миллионов лет
Запись цифр, заглавных и строчных латинских букв	1BAdf2...	10	3 года
	Dd1Dd1...	11	4 года
	1BBB1dfa...	13	5 лет
	S1fgf2D..	9	3 дня

Рисунок 5. Пароль, состоящий из цифр и строчных/заглавных букв, а также и из цифр, строчных и заглавных латинских букв

Таким образом, мы можем сделать вывод о том, что главным критерием в подборе надежного пароля является его длина: чем длиннее пароль, тем выше его безопасность; использование разных символов значительно повысит уровень сложности пароля; количество разных символов, а также типов в отдельности не влияет на время взлома.

Список литературы

1. Сервис, «HOW SECURE IS MY PASS-WORD?», https://www.security.org/how-secure-is-my-password/
2. Краткая история паролей от античности до наших дней. [Электронный ресурс]. − Режим доступа: https://habr.com/ru/company/selectel/blog/578578/
3. Парольная политика. [Электронный ресурс]. − Режим доступа: http://securitypolicy.ru