Пароли и аутентификация. Менеджеры паролей.

Олег Серов (Access Now)

Рейтинг самых слабых паролей - 2020 (nordpass.com)

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213
11. ↑ (12)	1234567	165,909	Less than a second	2,516,606

Как взламывают пароли

- Угадывание пароля (перебор по заданному множеству, перебор по словарю);
- Вычисление пароля по известной хэш-функции (нужен доступ к серверу аутентификации, где хранятся хэши)
- Перехват пароля (например, посредством фишинга)
- Компрометация одного из нескольких сервисов пользователя с совпадающими паролями

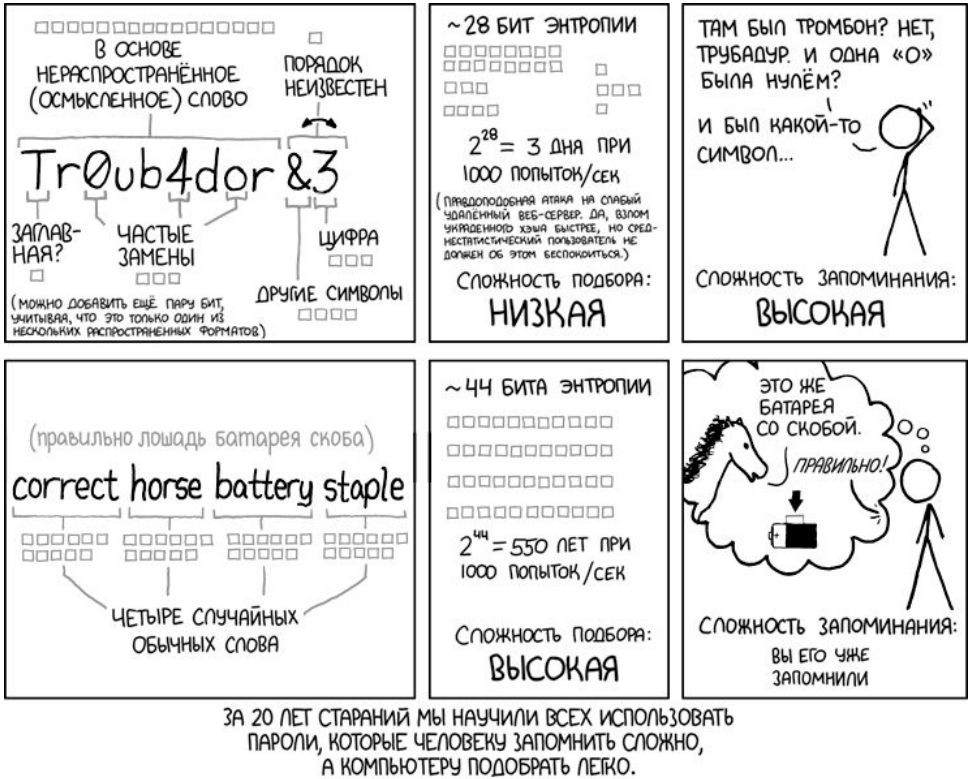
Сложность (сила, стойкость) пароля

- Сложность пароля оценивается как время, необходимое злоумышленнику для его подбора (либо как среднее количество попыток угадывания до первой успешной)
- Сложность пароля зависит от:
  - Длины пароля,
  - Используемого набора символов (алфавита),
  - Меры случайности при создании парольной последовательности

Общие рекомендации к сложности паролей

- Минимально рекомендуемая длина пароля — 12-14 символов.
- Рекомендуется генерировать случайные пароли (программный или аппаратный генератор “случайности”)
- Избегать использования паролей, содержащих словарные слова («sometext»), повторяющиеся наборы букв («oneoneone»), только буквенные или числовые последовательности («aaa», «123»), любые данные как либо ассоциированные с владельцем пароля.
- Рекомендуется включать в пароль одновременно цифры, алфавитные символы в разных регистрах, и специальные символы, если это разрешено системой.
- Рекомендуется избегать использования одного пароля для различных сайтов или целей (требование уникальности)

Использование парольных фраз



- Случайная последовательность слов, созданная генератором
- Более удобна для запоминания, благодаря ассоциативному ряду

Использование менеджера паролей

Менеджер паролей - это специальная программа, которая создаёт и хранит пароли.

- создают пароли, которые невозможно отгадать человеку,
- надёжно хранят пароли (и ответы на секретные вопросы),
- с помощью главного мастер-пароля (или парольной фразы) защищают все ваши пароли.

Примеры программ - менеджеров паролей

- KeePass
- KeePassXC
- LastPass
- 1Password
- Bitwarden

Факторы аутентификации

- Знание
- Обладание
- Неотъемлемая часть субъекта
- Местоположение субъекта