УДК 004.056

В. О. Клименко

АНАЛІЗ ЗАСОБІВ ЗАХИЩЕНОГО ЗБЕРІГАННЯ ПАРОЛІВ

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто ознаки слабких паролів та наведено їх приклади. Визначено поняття менеджеру паролів та доведено необхідність його використання. Створено таблицю порівняльного аналізу відомих менеджерів паролів.

Ключові слова: пароль, злам паролів, менеджер паролів, багатофакторна автентифікація, шифрування.

Abstract

The features of weak passwords are described and their examples are given at the work. Concept of a password manager is defined and the necessity of its usage is proven. The comparative analyses table of known password managers is designed.

Keywords: password, password breaking, password manager, multifactor authentication, encryption.

Вступ

На сьогоднішній день однією з основних проблем в захисті інформаційних систем від злому є використання слабких паролів. Більшість звичайних користувачів не приділяють достатньої уваги при створенні паролів, а деякі розробники перекладають відповідальність за створення паролів на користувачів, навіть, не надаючи ніяких рекомендацій [1, 2]. Таким чином перед працівниками з кібербезпеки та захисту інформації постає задача керування безпекою паролів. Саме тому актуально створювати засоби для керування захищеного зберігання паролів [2], до яких, зокрема, належать менеджери паролів.

Метою даного дослідження є підвищення рівня керування безпекою паролів шляхом застосування менеджерів паролів.

Аналіз стійкості паролів

Часто при створенні паролів користувачі використовують особисту інформацію таку, як: ім’я та прізвище, дата народження, або іншого важливого в їх житті дня [1]. Дану інформацію доволі легко отримати, прослідкувавши за соціальними мережами користувачів.

Окрім особистої інформації, також використовують прості послідовності літер або цифр, наприклад, «12345», «54321», «abcde», «qwerty» і тощо [2]. Те саме відбувається, якщо при створенні паролю система вимагає від користувача використання спеціальних символів, для створення стійкішого паролю. Користувачі можуть нехтувати даною рекомендацією і просто додати в кінці паролю один спеціальний символ, частіше всього це «!», або послідовність спеціальних символів, що відповідає клавішам «12345» - «!@#$%» [1, 2].

Також популярними паролями є імена відомих людей, назви брендів, спортивних клубів, музикальних гуртів, книжок, фільмів і т. д. Але всі ці паролі поступаються одному особливому. Відповідно до рейтингу 200 найбільш простих паролів від NordPass [3], самим популярним паролем є «password», що є перекладом слова «пароль» на англійську мову. Його було застосовано майже 5 мільйонів разів тільки за 2022 рік, а для його злому необхідно менше однієї секунди. Вся ця інформація використовується при створенні словників для зламу паролів. При цьому паролі залишаються найбільш вживаним фактором як однофакторної, так і багатофакторної автентифікацій.

Аналіз актуальності застосування менеджерів паролів

Менеджер паролів – це інструмент, що використовується для генерації, зберігання та спрощення використання паролів. Оскільки, в інтернеті існує багато сайтів та онлайн сервісів, де потрібна реєстрація, правильним буде не тільки використання надійного паролю, але й створення різних паролів для кожного сайту. Звісно утримати стільки паролів в голові дуже важко, тим паче, що ще однією рекомендацією щодо створення стійкого паролю є його регулярна заміна [1]. Саме тому більш простим і правильним буде використання менеджеру паролів. Даний інструмент створює стійкі паролі і зберігає їх у зашифрованому вигляді.

Головним недоліком використання менеджерів паролів є те, що, зламавши менеджер паролів, зловмисник отримає доступ до всіх облікових записів користувача. Тому, окрім створення надійного майстер паролю (master password) для даного інструмента, перевагою буде використання багатофакторної автентифікації.

Порівняльний аналіз відомих менеджерів паролів

Для аналізу було обрано 8 популярних менеджерів паролів:

1. NordPass[4].
2. RoboForm[5].
3. 1Password[6].
4. Keeper[7].
5. Dashlane[8].
6. LastPass[9].
7. Bitwarden[10].
8. Enpass[11].

В таблиці 1 наведено результати аналізу обраних менеджерів паролів та їх властивості.

Таблиця 1 – Результати порівняльного аналізу менеджерів паролів

	NordPass	RoboForm	1Password	Keeper	Dashlane	LastPass	Bitwarden	Enpass
Обмеження для безкоштовної версії	Для одного пристрою	Відсутня можливість резервного копіювання в хмару	Тільки платна	Тільки для мобільного пристрою	Для одного пристрою	Синхронізація між пристроями одного типу	Відсутній TOTP автентифікатор та можливість шифрування файлів	25 паролів для мобільної версії
Багатофакторна автентифікація	+	В платній версії	В платній версії	+	+	+	+	+
Біометричний вхід	+	+	В платній версії	+	+	+	+	+
Заповнення форм	+	+	В платній версії	+	+	+	+	+
Генератор паролів	+	+	В платній версії	+	+	+	+	+
Аварійний доступ	В платній версії	В платній версії	В платній версії	В платній версії	–	В платній версії	В платній версії	–
Надійність паролю	В платній версії	+	В платній версії	В платній версії	+	+	+	+
Шифрування	AES 256 bits	AES 256 bits	AES 256 bits	AES 256 bits	AES 256 bits	AES 256 bits	AES 256 bits	AES 256 bits
Платформи	Windows, Mac, iOS, Android, Linux	Windows, Mac, iOS, Android, Linux	Windows, Mac, iOS, Android. Linux	Windows, Mac, iOS, Android, Linux	Windows, Mac, iOS, Android, Linux	Windows, Mac, iOS, Android, Linux	Windows, Mac, iOS, Android, Linux	Windows, Mac, iOS, Android, Linux
Браузери	Chrome, Firefox, Safari, Edge, Brave, Opera	Chrome, Firefox, Safari, Edge, IE	Chrome, Firefox, Safari, Edge, Brave	Chrome, Firefox, Safari, Edge, IE, Opera	Chrome, Firefox, Safari, Edge, IE	Chrome, Firefox, Safari, Edge, Opera	Chrome, Firefox, Safari, Edge, Brave, Opera, Vivaldi, Tor	Chrome, Firefox, Safari, Edge, Opera, Vivaldi

З таблиці 1 можна зробити такі висновки:

- У всіх менеджерів паролів, окрім 1Password є безкоштовна версія;
- Всі менеджери паролів мають функції багатофакторної автентифікації, біометричного входу, заповнення форм, генерації паролів і перевірку стійкості паролів;
- Всі менеджери паролів, окрім Dashlane та Enpass, мають можливість аварійного доступу до облікового запису, хоча ця функція є тільки в платних версіях;
- Всі менеджери паролів використовують симетричне шифрування AES з 256-бітним ключем, яке є більш швидким, але не має математичного доведення стійкості порівняно з асиметричними алгоритмами, що не дозволяє виключити ризик його зламу у майбутньому;
- Всі менеджери паролів є кросплатформеними, хоча багато з них обмежені однією платформою в безкоштовній версії;
- Всі менеджери паролів підтримують багато популярних браузерів;
- RoboForm має можливість резервного копіювання в хмару, але в платній версії.

Таким чином, розробка нового менеджеру паролів повинна покращувати шифрування та включати основні функціональні можливості, притаманні відомим засобам.

Висновки

У даній роботі розглянуто ознаки слабких паролів, наведено їх приклади та надано рекомендації для створення стійких паролів. Визначено поняття менеджеру паролів та доведено необхідність його використання. Створено порівняльну таблицю відомих менеджерів паролів, яка дозволила визначити шляхи їх покращення з точки зору мети даного дослідження, а також множину функціональних можливостей засобів, які необхідні для того, щоб новий засіб був конкурентним.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Shannon Riley. Password Security : What Users Know and What They Actually Do. *Usability News*. 2006. Vol. 8, Issue 1. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.597.5846&rep=rep1&type=pdf (accessed: 10.03.2023).
2. Баришев Ю. В., Чайкін М. М., Кохан О. В.. Метод та засіб підвищення стійкості зрозумілих користувачам текстових паролів. *Наукові праці ВНТУ*. 2022. № 2. URL: https://praci.vntu.edu.ua/index.php/praci/article/view/655 (дата звернення: 10.03.2023).
3. NordPass – Top 200 most common passwords. URL: https://nordpass.com/most-common-passwords-list/ (accessed: 10.03.2023).
4. NordPass – NordPass features. URL: https://nordpass.com/features/ (accessed: 10.03.2023).
5. RoboForm – RoboForm features. URL: https://www.roboform.com/en/key-features (accessed: 10.03.2023).
6. 1Password – 1Password pricing. URL: https://1password.com/teams/pricing/ (accessed: 10.03.2023).
7. Keeper – Keeper Unlimited Free Trial & Keeper Free Version. URL: https://www.keepersecurity.com/free-trial-vs-free-version.html (accessed: 10.03.2023).
8. Dashlane – Trusted Personal Password Manager. URL: https://www.dashlane.com/personal-password-manager (accessed: 10.03.2023).
9. LastPass – Why LastPass. URL: https://www.lastpass.com/why-lastpass (accessed: 10.03.2023).
10. Bitwarden – Bitwarden pricing. URL: https://bitwarden.com/pricing/business/ (accessed: 10.03.2023).
11. Enpass – Enpass pricing. URL: https://www.enpass.io/pricing/ (accessed: 10.03.2023).

Клименко Володимир Олександрович – студент групи 1БС-19б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vovaklim2000@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця. email: yuriy.baryshev@vntu.edu.ua

Volodymyr Klymenko – student of 1БС-19б group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vovaklim2000@gmail.com

Scientific supervisor: ***Yurii Baryshev*** – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia. email: yuriy.baryshev@vntu.edu.ua