УДК 004.056

О. В. Кохан
Ю. В. Баришев

ЗАСІБ ГЕНЕРУВАННЯ СТІЙКОГО ПАРОЛЯ

Вінницький національний технічний університет

Анотація

Розглянуто важливість генерування якісного пароля на основі ключового слова користувача. Проаналізовано відомі методи розв'язання даної задачі. Запропоновано структуру програмного модуля для генерування стійких паролів.

Ключові слова: генерування паролів, стійкий пароль, автентифікація, авторизація

Abstract

The impact of proper password generating based on user key word. Known methods of this task solving were analyzed. A structure of software module for proper password generation was proposed.

Keywords: password generation, persistent password, authentication, authorization.

Вступ

Наразі проблема генерування стійких паролів, що будуть зрозумілими і запам'ятовуватимуться користувачу, є особливо актуальним. В кожного користувача, як мережі Інтернет, так і звичайного користувача персонального комп'ютера, існує необхідність захисту персональних даних. Одним з найпростіших методів автентифікації є автентифікація на основі знання певного секрету. Найбільш вживаним випадком такого секрету виступає пароль. Відомі, навіть, підходи де стійкість захисту обміну даними суттєво залежить від вдалого вибору пароля користувачем [1, 2]. Проте даний метод може бути доволі просто зламаний методом підбору пароля за спеціальними словниками чи навіть грубим методом перебору символів-літер [3, 4]. Для збільшення стійкості паролів, ключове слово повинно містити якомога більше різноманітних символів, що дозволить ускладнити зловмисникам отримати доступ до персональних даних. Водночас можливість запам'ятовування складних паролів, згенерованих випадковим чином, що можуть налічувати понад 10 символів, стає складною задачею для користувачів. Це може призвести до втрати даних, доступ до яких визначався цим паролем. Тому більшість людей жертвують надійністю захисту своїх даних. Саме тому виникає необхідність створення програмного засобу, який дозволить за обраним користувачем ключовим словом створити якомога стійкіший пароль, який для користувача буде нескладно запам'ятати.

Метою є покращення стійкості пароля без суттєвої втрати його легкості до запам'ятовування користувачем.

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати доступні генератори захищених паролів;

- визначити вимоги до стійкості паролів;
- обрати підхід до перетворення зрозумілих слів у стійкий пароль;
- підібрати мову та середовище програмування;
- програмна реалізація задачі;
- налагодити та протестувати застосунок;
- проаналізувати результати.

Результати дослідження

Для створення програмного засобу, що буде генерувати захищені паролі, необхідно визначити вимоги щодо їх стійкості. Оскільки застосунок призначений для звичайних користувачів, то мінімальна довжина паролю повинна складати не менше восьми символів. Також пароль повинен містити символи щонайменше із трьох таких груп [3]:

- латинські літери: abcd...xyz;
- латинські літери у верхньому регістрі: ABCD...XYZ;
- цифри: 123…90;
- спеціальні символи: !#@_+ тощо.

Використовуючи вище наведені вимоги, можна згенерувати стійкий пароль. Однак наразі в мережі Інтернет генератори паролів достатньо поширені. Зазвичай вони представлені онлайн-інструментами, призначеними для генерування паролів із заданими параметрами. Відтак користувач може вказати необхідну довжину пароля та набори символів, що будуть входити в нього. Також часто трапляються генератори паролів в сукупності з менеджерами паролів. Зазвичай це браузерний застосунок, що генерує за користувача пароль, прив’язує його до відповідного облікового запису чи ідентифікатора та вводить в потрібний момент [4]. Зазвичай згенеровані таким чином паролі можуть вважатися стійкими, проте такі генератори створюють ключові слова, що неможливо запам’ятати – набір відповідних символів вказаної кількості. Якщо при цьому згадати, що відповідно до рекомендацій безпеки паролі необхідно час-від-часу оновлювати, то постає проблема для користувачів, яка радше за все буде розв’язана не на користь правил кібербезпеки.

Більше того, при зупинці роботи такого сервісу або його деінсталяції чи інших причин, доступ до облікових записів буде втрачено, як і персональні дані, що захищалися цими паролями. А запис таких парольних комбінацій в іншому файлі чи на папері може призвести до розсекречення паролів. Тому відомі онлайн-сервіси чи застосунки для генерування паролів, хоча й створюють стійкий пароль, подальше його використання ускладнюється і може призвести до небажаних наслідків.

Для вирішення цієї задачі пропонується інший підхід до генерування паролю. Користувач сам обирає та вводить ключове слово, яке послужить основою для генерації стійкого паролю. Програмний застосунок має аналізувати введено слово та замінювати його окремі літери спеціальними символами та "розбавлятиме" цифрами, що і буде ускладнювати пароль. Такий метод дозволить користувачу в певній мірі самому обирати пароль та буде надавати можливість запам’ятати пароль самостійно, а не за допомогою програмного застосунку, що дозволить вирішити проблеми з втратою облікових записів і даних.

Запропонований засіб повинен складатися з таких модулів:

- бібліотека правил заміни символів;

- блок аналізу стійкості пароля;

- блок ускладнення пароля;

- інтерфейс користувача.

Задача бібліотеки випливає з її назви – заміняти символи, які вводить користувач на менш прогнозовані, але очевидні користувачеві. У випадку, коли лише роботи такої бібліотеки буде недостатньо внаслідок специфіки обраного користувачем слова як пароля, передбачається виклик блоку ускладнення пароля, який буде додавати символи в пароль, якщо блок аналізу стійкості видасть невідповідність поточного його варіанту критеріям стійкості.

Висновки

Аналіз існуючих генераторів паролів показав, що попри їх велику кількість, вони недостатньо різноманітні з точки зору алгоритму генерування пароля. Крім того, вони мають недолік, пов'язаний зі складністю запам'ятовування згенерованого пароля користувачем, що на практиці обумовлює порушення найкращих практик щодо організації політики безпеки стосовно паролів. Саме тому запропоновано підхід, який дозволить забезпечити компроміс між стійкістю та зручністю запам'ятовування. Для реалізації даного підходу розроблено структуру програмного застосунку та описано його основні функціональні блоки.

СПИСОК ВИКОИСТАНОЇ ЛІТЕРАТУРИ

1. Баришев Ю. В., Каплун В. А. Метод автентифікації віддалених користувачів для мережевих сервісів. Інформаційні технологій та комп'ютерна інженерія. 2014. №2. С. 13-17.
2. Y. Baryshev, V. Kaplun, K. Neuimina. Discretional model and method of distributed information resources access control. Scientific Works of Vinnytsia National Technical University. 2017. №2. 8 p. URL: https://works.vntu.edu.ua/index.php/works/article/download/504/505 (accessed 09.03.2020)
3. Парольна защита. Инструкция по организации [Електронний ресурс]. URL: https://compnote.ru/otdelit/instruktsiya-po-organizatsii-parolnoy-zashhityi/ (дата звернення 09.03.2020)
4. Лучшие генераторы паролей для защиты от взлома [Електронний ресурс]. Режим доступу URL: https://lifehacker.ru/generatory-parolej/ (дата звернення 09.03.2020)

Кохан Олександр Володимирович - студент групи 1БС-16б, факультет інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail : sasha.kohan98@gmail.com
Баришев Юрій Володимирович – к. т. н. доцент кафедри захисту інформації, , Вінницький національний технічний університет, Вінниця

Alexander Kohan - student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University: sasha.kohan98@gmail.com
Yurii Baryshev – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, email: yuriy.baryshev@vntu.edu.ua