Menedżery Haseł

Kamil Kozioł, Magdalena Sadowska, Wiktor Leszczyński

1 Wstęp

Raport ma na celu przedstawienie konceptu menadzerow hasel, przeglad dostepnych rozwiazan oraz prezentacje wlasnej implementacji. Dokument zostal stworzony na potrzeby przedmiotu Wprowadzenie do Cyberbezpeczenstwa.

1.1 Czym jest password menager?

1.1.1 Zastosowanie

1.1.2 Zalozenia

2 Menedżery

Istnieje wiele innych menedżerów haseł, które oferują różne funkcje i poziomy bezpieczeństwa. Wybór konkretnego menedżera haseł zależy od indywidualnych preferencji użytkownika i wymagań dotyczących bezpieczeństwa danych.

2.1 Wybrane menadzery

Lista wybranych menadzerow, które zostaną przedstawione:

- LastPass,
- 1Password,
- NordPass,
- KeePassXC,

	Google Password Manager	Dashlane
Platformy	Windows, macOS, Android, iOS	Windows, macOS, Android, iOS, Linu
Aplikacja mobilna	Natywna funkcja Androida	Android, iO
Generator haseł	Tak	Tak
Wtyczki	Natywna funkcja Chrome	Chrome, Firefox, Opera
Szyfrowanie	AES 256	AES 256 z SBC-I
Klucz sprzętowy	Tak	Tak
Synchronizacja Multiplatformowa	Tak	Tak
Eksport i import .csv	Tak	Tak
Licencje i plany	Freeware	Darmowy Premium (3,99 USI Family (5,99 USD

- BitWarden.

2.1.1 LastPass

Jest to jedna z najpopularniejszych aplikacji do przechowywania haseł. LastPass umożliwia przechowywanie haseł, kart kredytowych i innych danych w chmurze, a także generowanie mocnych haseł i automatyczne wypełnianie formularzy.

2.1.2 Wady

2.1.3 Zalety

2.2 1Password

Wieloplatformowy menedżer haseł, którego producentem jest przedsiębiorstwo AgileBits, możliwia przechowywanie haseł, kart kredytowych i innych danych w chmurze. 1Password jest płatnym oprogramowaniem zamkniętym na licencji shareware. Aplikacja korzysta z funkcji haszującej PBKDF2 i szyfruje dane przy użyciu 256-bitowego algorytmu AES. W celu zwiększenia bezpieczeństwa stosowana jest również weryfikacja dwuetapowa.

2.2.1 Wady

- Płatny

2.2.2 Zalety

- Synchronizacja z chumrą
- Możliwość przechowywania dokumentów, obrazów i innych plików
- W przypadku zgubienia Tajnego klucza nie można wygenerować nowego i konieczne jest utworzenie nowego konta

2.3 NordPass

2.3.1 Wady

2.3.2 Zalety

2.4 KeePassXC

Został stworzony przez KeePassXC Team, jest bezplatnym narzedziem open source, ktore dziala na licencji GLP 2.0 i 3.0. Powstal on jako widelec KeePassX, ktory przestal byc rozwijany. Baza danych jest szyfrowana za pomocą algorytmu AES256 lub szyfru blokowego Twofish, a nastepnie jest uzyta funkcja haszowana. Mozna dodatkowo zabezpieczyc baze plikiem-kluczem wypelnionym dowolna iloscia losowych bajtow lub uzywajac YubiKey.

2.4.1 Wady

- Brak wbudowanej synchronizacji z chmura,
- Zlozony interfejs,
- Brak dedykowanej aplikacji mobilnej.

2.4.2 Zalety

- Open source,
- Dwuskladnikowe uwierzytelnianie,
- Funkcja Auto-Type, automatycznie wpisuje nazwę użytkownika i hasło w formularzach.

2.5 BitWarden

Bezpłatny menedżer haseł, który oferuje szyfrowanie end-to-end i dwuskładnikową autoryzację. Bitwarden umożliwia także przechowywanie danych karty kredytowej i wypełnianie formularzy.

2.5.1 Wady

2.5.2 Zalety

3 Metody zabezpieczania sejfów

3.1 Metody szyfrowania sejfu

Menedżery haseł zapewniają bezpieczne przechowywanie haseł i innych poufnych danych dzięki zastosowaniu zaawansowanych algorytmów szyfrowania z których najczęściej stosowane to:

- Advanced Encryption Standard (AES) – jest to jeden z najbezpieczniejszych i najpopularniejszych algorytmów szyfrowania stosowanych przez menedżery haseł. AES działa na blokach danych o długości 128 bitów i wykorzystuje klucz szyfrowania o długości 128, 192 lub 256 bitów.
- Blowfish – jest to szybki i skuteczny algorytm szyfrowania stosowany przez menedżery haseł. Blowfish działa na blokach danych o długości 64 bitów i wykorzystuje klucz szyfrowania o długości od 32 do 448 bitów.
- Twofish – to inny popularny algorytm szyfrowania stosowany przez menedżery haseł. Twofish działa na blokach danych o długości 128 bitów i wykorzystuje klucz szyfrowania o długości 128, 192 lub 256 bitów.

3.2 AES

3.2.1 Historia

AES (Advanced Encryption Standard) jest to symetryczny szyfr blokowy oparty na algorytmach Rijndaela, storzonych w 1998 w ramach konkursu gdzie zostały zaprezentowane Instytucji NIST. Na ich podstawie wybranych algorytów powstał AES będący następcą algorytmu DES.

3.2.2 Działanie

AES działa na stałej długości bloków (128 bitów) i używa tajnego klucza, który może przyjąć długości 128, 192, 256 bitów. Cechuje się wysoką wydajnością zarówno w przypadku sprzętu komputerowego, jak i oprogramowania. AES opiera się na zasadzie znanej jako sieć substytucji-permutacji. W odróżnieniu od swojego poprzednika, czyli algorytmu DES, AES nie korzysta z Sieci Feistela. Algorytm operuje na macierzy bajtów o wymiarach 4×4, nazywaną stanem. Jednak niektóre wersje algorytmu dysponują większym rozmiarem bloku oraz dodatkowymi kolumnami w macierzy.

Rozmiar klucza używany w algorytmie określa liczbę powtórzeń transformacji, które przekształcają dane wejściowe (czyli tekst jawny) w dane wyjściowe (szyfrogram). Liczba cykli powtórzeń jest następująca:

10 cykli powtórzeń dla klucza 128-bitowego. 12 cykli powtórzeń dla klucza 192-bitowego. 14 cykli powtórzeń dla klucza 256-bitowego. Wszystkie rundy składają się z kilku kroków, z których każdy rozłożony jest na cztery podobne etapy.

Wykonując operacje w odwrotnej kolejności używając tego samego klucza, można przekształcić szyfrogram z powrotem w tekst jawny.

3.3 Blowfish

3.4 Twofish

3.4.1 Historia

Twofish to algorytm szyfru blokowego z kluczem symetrycznym, który został zaprojektowany przez Bruce'a Schneiera, Johna Kelseya, Douga Whitinga, Davida Wagnera, Chrisa Halla i Nielsa Fergusona w 1998 roku. Jest to następca algorytmu szyfrowania Blowfish.

3.4.2 Działanie

Twofish działa na blokach danych o stałej długości (128 bitów) i używa tajnego klucza do szyfrowania i deszyfrowania danych. Długość klucza może wynosić od 128 do 256 bitów, co czyni go bardziej bezpiecznym niż Blowfish.

Algorytm Twofish wykorzystuje strukturę sieci Feistela, która jest powszechnie stosowaną strukturą w szyfrach blokowych. Polega on na podzie-

leniu danych wejściowych na dwa równej wielkości bloki, a następnie zastosowaniu serii rund do bloków przy użyciu harmonogramu klucza.

Podczas każdej rundy, nieliniowa funkcja substytucji (S-box) jest stosowana do każdego bloku, aby wprowadzić zamieszanie, a liniowa transformacja (macierz MDS) jest stosowana do każdego bloku, aby wprowadzić dyfuzję. Harmonogram klucza jest używany do generowania zestawu kluczy okrągłych z oryginalnego tajnego klucza, które są używane w każdej rundzie do modyfikacji danych wejściowych.

Jedną z kluczowych mocnych stron Twofish jest jego zależne od klucza S-boxy, które sprawiają, że jest bardziej odporny na niektóre ataki, takie jak kryptoanaliza różnicowa. Ma również silny efekt lawinowy, co oznacza, że niewielka zmiana w danych wejściowych lub kluczu powoduje znaczącą zmianę w danych wyjściowych.

Został on przyjęty przez kilka organizacji zajmujących się standardami bezpieczeństwa, w tym Narodowy Instytut Standardów i Technologii (NIST) oraz Międzynarodową Organizację Normalizacyjną (ISO). Szyfr Twofish nie zostal opatentowany.

Wszystkie powyższe algorytmy szyfrowania są uważane za bardzo bezpieczne i wykorzystywane przez wiele menedżerów haseł. Ponadto, menedżery haseł często stosują dodatkowe zabezpieczenia, takie jak hasła główne, dwuskładnikową autoryzację (np. TOTP, UbiKey) i szyfrowanie końcowe do ochrony danych użytkownika.

3.5 Metody hashowania haseł głównych

- PBKDF2 (Password-Based Key Derivation Function 2) – jest to algorytm hashowania, który wykorzystuje iteracyjny proces szyfrowania w celu zwiększenia bezpieczeństwa hasła głównego. PBKDF2 wykorzystuje funkcję skrótu, która generuje wartość hasha na podstawie hasła użytkownika, a następnie przeprowadza iteracyjny proces szyfrowania w celu uzyskania klucza szyfrującego. Proces ten jest powtarzany wielokrotnie, co zwiększa trudność w łamaniu hasła głównego.

- Bcrypt – jest to inny popularny algorytm hashowania, który jest bardzo bezpieczny i trudny do złamania. Bcrypt wykorzystuje funkcję skrótu, która generuje wartość hasha na podstawie hasła użytkownika i soli, która jest dodawana do hasha w celu zwiększenia bezpieczeństwa. Bcrypt jest również iteracyjny i wykorzystuje różne parametry, takie

jak koszt, który określa, jak długo ma trwać proces hashowania.

- Scrypt – jest to algorytm hashowania, który został opracowany specjalnie do ochrony haseł przed atakami typu brute force i słownikowymi. Scrypt wykorzystuje funkcję skrótu, która generuje wartość hasha na podstawie hasła użytkownika i soli, a następnie przeprowadza iteracyjny proces szyfrowania w celu uzyskania klucza szyfrującego. Proces ten jest powtarzany wielokrotnie, co utrudnia atakującym łamanie hasła głównego.

4 Przyszłość menedżerów haseł

4.1 WebAuthn

Web Authentication (WebAuthn) to otwarty standard W3C, który umożliwia uwierzytelnianie użytkowników bez używania tradycyjnych haseł. Wykorzystywana jest kryptografia asymetryczna, która polega na zastosowaniu kluczy publicznych i prywatnych. Aby skorzystać z WetAuthn, użytkownik musi najpierw zarejestrować swoje klucze w usłudze internetowej, którą chce używać. Bezpieczne klucze mogą być zapisane na fizycznych urządzeniach, takich jak klucze USB lub karty inteligentne, lub mogą być generowane na podstawie biometrii. Klucz publiczny jest zaszyfrowany i przechowywany na serwerze, a klucz prywatny znajduje się lokalnie na urządzeniu użytkownika. Co istotne, standard ten jest obsługiwany przez większość dostępnych przeglądarek internetowych, co umożliwia jego szerokie zastosowanie.

Podczas procesu uwierzytelniania, usługa internetowa wysyła zapytanie do urządzenia użytkownika, aby potwierdzić tożsamość użytkownika. Użytkownik potwierdza swoją tożsamość, używając bezpiecznego klucza, który jest przechowywany na urządzeniu. Urządzenie użytkownika następnie przekazuje odpowiednie informacje zwrotne do usługi internetowej, potwierdzając tożsamość użytkownika.