

CZY TO JUŻ KONIEC HASEŁ?

Jarosław Biszczuk, Bartłomiej Krowiak
Ośrodek Edukacji Informatycznej i Zastosowań Komputerów
w Warszawie, Raszyńska 8/10
{jaroslaw.biszczuk, bartlomiej.krowiak}@oeiizk.edu.pl

Abstract. *This article addresses critical aspects of authentication in computer systems and network services, focusing on enhancing digital security beyond traditional passwords. It explores modern techniques such as password managers, multi-factor authentication (MFA), and passwordless logins using passkeys and hardware security keys. The aim is to raise awareness and provide practical knowledge for effective data protection in the digital realm.*

1. Wstęp

Uwierzytelnianie w systemach komputerowych lub usługach sieciowych jest jednym z kluczowych aspektów cyfrowego bezpieczeństwa. Uzyskanie danych logowania np. za pomocą ataku phishingowego jest z kolei głównym wektorem ataku na usługę lub system komputerowy. Dlatego ważna jest świadomość istnienia różnych technik zabezpieczeń oraz ich charakterystyki.

2. Menedżer haseł

Częstą praktyką użytkowników jest używanie tego samego hasła do logowania w różnych serwisach. Wyciek danych logowania z jednego serwisu powoduje narażenie w innych usługach. Dobrą praktyką administratorów serwisów jest przechowywanie nie samych haseł, lecz ich skrótów kryptograficznych (hash). Po nieautoryzowanym uzyskaniu dostępu do takiego skrótu konieczne jest jeszcze znalezienie hasła w postaci jawnej (plaintext). Programy, które obliczają skróty z generowanych haseł i porównują z haszem z wycieku, robią to z różnymi prędkościami – zależnie od użytego algorytmu. Popularne programy tego typu to między innymi **John the Ripper** i **Hashcat**.

Na rysunku 1 przedstawiono fragment testu z programu John the Ripper pokazujący szybkości obliczania skrótów dla kilku algorytmów. Na przykład skrót SHA-256 jest obliczany z prędkością blisko 63 milionów haseł w ciągu sekundy na 12 rdzeniowym procesorze. Użycie kart graficznych do obliczania skrótów znacząco zwiększa tę liczbę.

```
C:\Windows\System32\cmd.e x + v
Benchmarking: Raw-Blake2 [BLAKE2b 512 128/128 AVX]... (12xOMP) DONE
Raw: 21101K c/s real, 2638K c/s virtual

Benchmarking: Raw-Keccak [Keccak 512 32/64]... (12xOMP) DONE
Raw: 12969K c/s real, 1348K c/s virtual

Benchmarking: Raw-Keccak-256 [Keccak 256 32/64]... (12xOMP) DONE
Raw: 14459K c/s real, 1334K c/s virtual

Benchmarking: Raw-MD4 [MD4 256/256 AVX2 8x3]... DONE
Raw: 102299K c/s real, 102299K c/s virtual

Benchmarking: Raw-MD5 [MD5 256/256 AVX2 8x3]... DONE
Raw: 86257K c/s real, 85816K c/s virtual

Benchmarking: Raw-MD5u [md5(utf16($p)) 256/256 AVX2 8x3]... DONE
Raw: 84307K c/s real, 84804K c/s virtual

Benchmarking: Raw-SHA1 [SHA1 256/256 AVX2 8x]... DONE
Raw: 44531K c/s real, 45191K c/s virtual

Benchmarking: Raw-SHA1-AxCrypt [SHA1 256/256 AVX2 8x]... DONE
Raw: 44442K c/s real, 44739K c/s virtual

Benchmarking: Raw-SHA1-LinkedIn [SHA1 256/256 AVX2 8x]... DONE
Raw: 43890K c/s real, 43804K c/s virtual

Benchmarking: Raw-SHA224 [SHA224 256/256 AVX2 8x]... (12xOMP) DONE
Raw: 48794K c/s real, 8539K c/s virtual

Benchmarking: Raw-SHA256 [SHA256 256/256 AVX2 8x]... (12xOMP) DONE
Raw: 62830K c/s real, 11339K c/s virtual

Benchmarking: Raw-SHA3 [SHA3 512 32/64]... (12xOMP) DONE
Raw: 13065K c/s real, 1390K c/s virtual

Benchmarking: Raw-SHA384 [SHA384 256/256 AVX2 4x]... (12xOMP) DONE
Raw: 31446K c/s real, 4577K c/s virtual

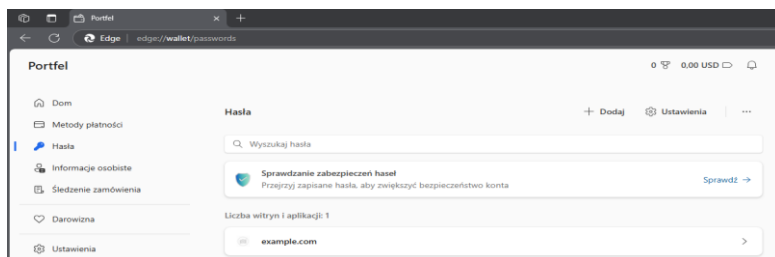
Benchmarking: ripemd-128, RIPEMD 128 [32/64]... DONE
Raw: 8346K c/s real, 8533K c/s virtual
```

Rysunek 1. Uruchomienie programu John the Ripper poleceniem: `john --test`

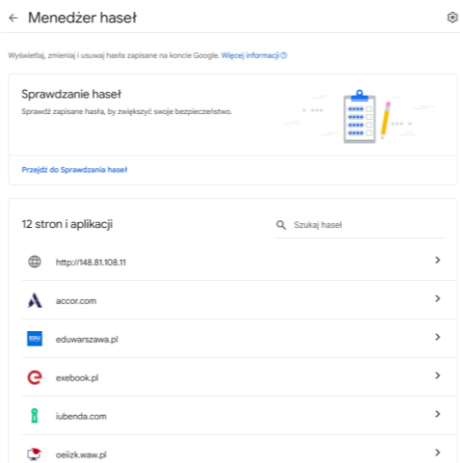
Wycieki danych logowania z serwisów, które upubliczniono, można sprawdzać na stronie *Have I Been Pwned* [1]. Obecnie (czerwiec, 2025) jest tam dodanych blisko 15 mld danych o skompromitowanych kontach do różnych serwisów www.

Pierwszym krokiem w dbaniu o bezpieczeństwo jest nieużywanie tych samych haseł w różnych serwisach oraz wykorzystywanie menedżera haseł.

We wszystkich popularnych przeglądarkach istnieje mechanizm zapisywania haseł. Przechowywane są one lokalnie, a po skonfigurowaniu konta można też przechowywać je w chmurze. To drugie rozwiązanie pozwala na dostęp do zapamiętanych haseł z różnych komputerów.



Rysunek 2. Chmurowy menedżer haseł w Microsoft Edge



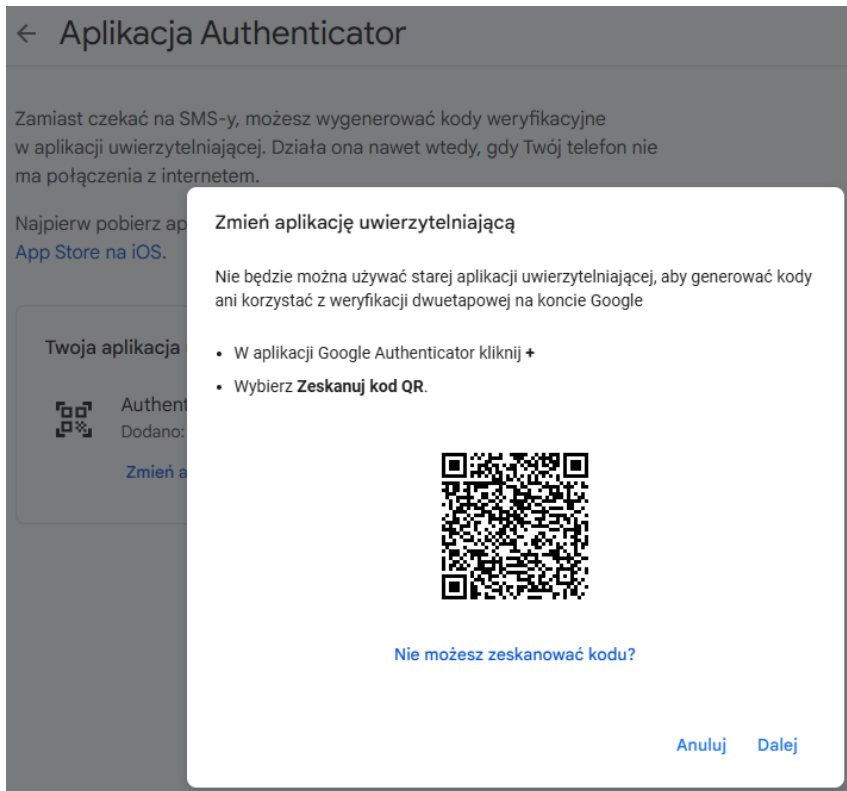
Rysunek 3. Chmurowy menedżer haseł w Google Chrome

Oprócz menedżerów wbudowanych w przeglądarkę dostępne są rozszerzenia oferujące dodatkowe funkcjonalności. Przegląd takich rozwiązań można znaleźć np. na stronie *The Best Free Password Managers of 2025* [5]. Wśród polecanych menedżerów warto zwrócić uwagę na **Bitwarden**. Przed wybraniem alternatywnego rozwiązania należy uważnie sprawdzić jego historię i reputację.

Często dane logowania zbierane są przez złośliwe oprogramowanie. Nie wszystkie są publikowane, na stronie wired.com można znaleźć informacje o jednym z ostatnich upublicznionych wycieków [4]. Przykład ten pokazuje, że nawet hasła trzymane w chmurze nie są bezpieczne na zainfekowanym komputerze.

3. Logowanie wieloskładnikowe

Samo hasło okazuje się niewystarczające. Jedną z technik zabezpieczających uwierzytelnianie jest użycie logowania dwuczynnikowego (2FA) zwanego też wieloskładnikowym (MFA). Najpopularniejszym rozwiązaniem (czynnikiem) w tej grupie zabezpieczeń jest używanie jednorazowych haseł opartych o czas (TOTP). Użytkownik za pomocą aplikacji skanuje kod QR, w którym jest m.in. losowy ciąg znaków (*sekret*). Zgodnie z publicznym standardem sekret składany jest z licznikiem zwiększanym w czasie. Następnie obliczany jest *skrót* (hash), z którego wybierane jest najczęściej 6 cyfr. Liczniki czasowe są zmieniane najczęściej co 30 sekund. Czas jest wymieniany w protokole komunikacyjnym, więc ustawienia czasu systemowego na komputerze i telefonie są nieistotne.



Rysunek 4. Kod QR do aplikacji Google Authenticator

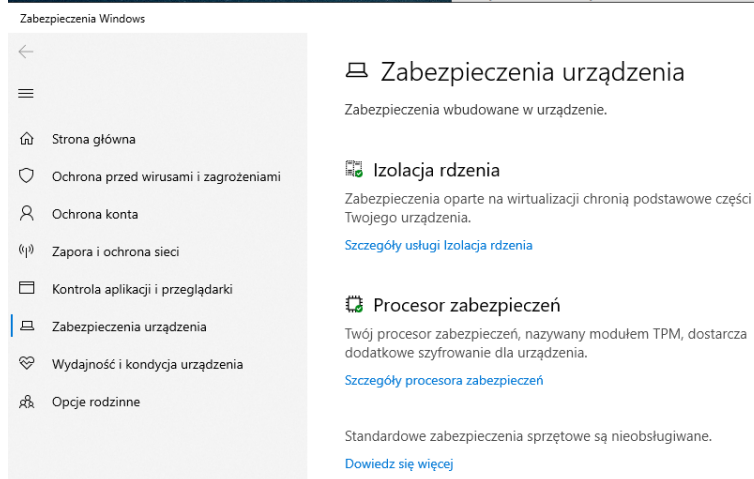
Na rysunku 4 widoczny jest przykładowy kod, który należy zeskanować telefonem w aplikacji Google Authenticator, Microsoft Authenticator lub innej, służącej do generowania kodów TOTP. Dekodując ten kod otrzymamy:

```
otpauth://totp/Google%3Ajaroslaw.biszczyk%40gsu-  
ite.dabrowski37lo.edu.pl?secret=  
3oqrf42hdd4cv76c3pdlr4feradi5ja2&issuer=Google
```

Sekret jest losowym 160 bitowym ciągiem zakodowanym w base32.

Innymi metodami uwierzytelniania wieloskładnikowego są wiadomości SMS oraz powiadomienia *push* na telefon. Korzystanie z nich wiąże się z koniecznością podania numeru telefonu w ustawieniach konta. Kolejną metodą jest wygenerowanie i użycie klucza dostępu (passkey). Jest on przypisany do komputera i jego wykradzenie przez złośliwe oprogramowanie nie jest problemem. Klucz jest zaszyfrowany za pomocą

modułu TPM w wersji 2.0, ale nie wszystkie komputery są wyposażone w ten układ. Po wyszukaniu w panelu sterowania frazy „zabezpieczenia urządzenia” na komputerze bez modułu TPM otrzymamy komunikat „Standardowe zabezpieczenia sprzętowe są nieobsługiwane”. Komunikat ten może też pojawić się, gdy podczas rozruchu komputera nie wykorzystano metody „Secure Boot”[6]



Rysunek 5. Informacje z komputera, na którym nie można uruchomić MFA z kluczem dostępem z komputera

Moduł TPM po odblokowaniu pinem, biometrią lub skanem twarzy pozwala na odszyfrowanie klucza (passkey). Klucze bez modułu TPM można zdefiniować w telefonie i uwierzytelniać za pomocą działającego Bluetooth na komputerze. Należy pamiętać, że klucz jest przypisany do telefonu i należy go ponownie wygenerować na nowym urządzeniu. Menedżer haseł nie przechowuje tych kluczy w odróżnieniu od sekretów TOTP, które są zapisywane na koncie.

4. Logowanie passwordless

Klucze dostępu używane jako drugi czynnik uwierzytelniania mogą także posłużyć do logowania bezhasłowego. Metoda ta zdobywa coraz większą popularność po zaimplementowaniu jej w popularnych serwisach. Pewną uciążliwością jest przechowywanie klucza dostępu tylko na jednym urządzeniu i generowanie kluczy dla każdego nowego urządzenia. Z pomocą przychodzą sprzętowe klucze bezpieczeństwa komunikujące się standardami USB lub NFC, które pozwalają na wygenerowanie i przechowywanie kilkunastu kluczy dostępu. W tym przypadku nie trzeba ich generować na różnych urządzeniach. Popularną marką takich kluczy jest Yubico SecurityKey. Informacje o konfiguracji klucza dostępu i/lub zabezpieczeń znajdziemy m.in. w Centrum pomocy

Google [3] oraz w Pomocy technicznej Microsoft [2]. Wiele serwisów udostępnia możliwość logowania za pomocą kluczy bezpieczeństwa. Na przykład podczas logowania do stron bankowych ipko.pl i ingbank.pl mamy możliwość zalogowania się za pomocą klucza i jest to traktowane jako jeden z czynników uwierzytelniania – nie można zrezygnować z hasła.

5. Podsumowanie

Opieranie się tylko na logowaniu hasłem jest anachroniczne i niebezpieczne – należy korzystać z innych form uwierzytelniania oraz znać charakterystykę tych metod. Przy uwierzytelnianiu za pomocą SMS możliwe są do przeprowadzenia ataki z tzw. SIM Swap. Możliwe są też scenariusze, polegające na tym, że do serwisu można uzyskać dostęp po przechwyceniu sesji przeglądarki (ang. *session hijacking*). Po zalogowaniu się, złośliwe oprogramowanie wykrada ciasteczka sesyjne i tokeny autoryzacyjne. Tu pomocne będzie wylogowanie się po każdej sesji, a nie bezpośrednie zamykanie okna przeglądarki.

Literatura

1. Have I Been Pwned, serwis umożliwiający sprawdzenie wycieku danych logowania, <https://haveibeenpwned.com>, ostatni dostęp 5.06.2025 roku.
2. *Logowanie się na koncie przy użyciu klucza zabezpieczeń*, Pomoc techniczna Microsoft, <https://tiny.pl/dw3tyy18>, ostatni dostęp 5.06.2025 roku.
3. *Logowanie się za pomocą klucza dostępu zamiast hasła*, Konto Google – Pomoc, <https://tiny.pl/yf1dh1vg>, ostatni dostęp 5.06.2025 roku.
4. *Mysterious Database of 184 Million Records Exposes Vast Array of Login Credentials*, WIRED, <https://tiny.pl/q8mcn6f1>, ostatni dostęp 5.06.2025 roku.
5. The Best Free Password Managers of 2025, lista bezpłatnych menedżerów hasel, <https://www.passwordmanager.com/best-free-password-managers>, ostatni dostęp 5.06.2025 roku.
6. Support for passkeys in Windows, <https://tiny.pl/3dwgdkx9>, ostatni dostęp 5.06.2025 roku.