**AKADEMIA NAUK STOSOWANYCH**

**W NOWYM SĄCZU**

**WYDZIAŁ NAUK INŻYNIERYJNYCH**

**PRACA DYPLOMOWA**

SYSTEMY UWIERZYTELNIANIA

**Autor: Rafał Michalik**

**Kierunek: Informatyka**

**Nr albumu: 30515**

**Promotor:** dr Grzegorz Surówka

**Akceptacja promotora: ……………………………………………………**  data i podpis

**NOWY SĄCZ 2024**

Spis treści

[1. Wprowadzenie 4](#_Toc153900403)

[2. Cel i zakres pracy 5](#_Toc153900404)

[3. Rozdział 1: Podstawy Systemów Uwierzytelniania 6](#_Toc153900405)

[3.1. Definicje i koncepcje podstawowe 6](#_Toc153900406)

[3.2. Historia rozwoju systemów uwierzytelniania 7](#_Toc153900407)

[3.3. Znaczenie i rola systemów uwierzytelniania w bezpieczeństwie informatycznym 8](#_Toc153900408)

[4. Rozdział 2: Klasyczne Metody Uwierzytelniania 10](#_Toc153900409)

[4.1. Uwierzytelnianie oparte na czymś, co się wie (wiedza) 10](#_Toc153900410)

[4.2. Uwierzytelnianie oparte na czymś, co się ma (posiadanie) 13](#_Toc153900411)

[5. Rozdział 3: Nowoczesne Technologie Uwierzytelniania 16](#_Toc153900412)

[5.1. Uwierzytelnianie biometryczne 16](#_Toc153900413)

[5.2. Uwierzytelnianie wieloskładnikowe (MFA) 18](#_Toc153900414)

[5.3. Uwierzytelnianie oparte na kryptografii 19](#_Toc153900415)

[6. Rozdział 4: Zagrożenia i Ryzyko w Systemach Uwierzytelniania 21](#_Toc153900416)

[6.1. Ataki na systemy uwierzytelniania 21](#_Toc153900417)

[6.2. Zabezpieczenia przed atakami 22](#_Toc153900418)

[7. Rozdział 5: Aplikacja do uwierzytelniania wieloskładnikowego 24](#_Toc153900419)

[7.1. Auth0 28](#_Toc153900420)

[8. Rozdział 6: Podsumowanie i Wnioski 30](#_Toc153900421)

[9. Bibliografia 31](#_Toc153900422)

# Wprowadzenie

W dzisiejszym świecie, w którym technologia odgrywa coraz większą rolę, problem bezpieczeństwa i uwierzytelniania ma kluczowe znaczenie. Nasze życie zależy w znacznym stopniu od technologii, cyfrowych usług oraz przetwarzania naszych danych. Wraz z tym wzrasta również zagrożenie dla naszych danych, cennych informacji, które w niepowołanych rękach mogą spowodować znaczące straty nie tylko finansowe ale także wizerunkowe. Współczesne społeczeństwo jest zdominowane przez technologie cyfrowe. Internet i urządzenia mobilne stały się nieodłączną częścią naszego życia codziennego. Korzystamy z sieci do komunikacji, pracy, zakupów, rozrywki i wielu innych celów. Wraz z tym wzrostem zależności od technologii, pojawiają się także nowe wyzwania związane z bezpieczeństwem i prywatnością.

Dlatego bardzo ważny jest stały wzrost mocy zabezpieczeń i kontroli osób czy też organizacji, które posiadają nasze dane, przetwarzają je i wykorzystują dla swoich celów.

Kontrola może następować w dwóch płaszczyznach: fizycznej i wirtualnej, i zazwyczaj są one wzajemnie powiązane. Przykładem takiego systemu jest czytnik odcisku linii papilarnych zamontowany między innymi w urządzeniach mobilnych. Po fizycznym sczytaniu odcisku palca weryfikuje jego poprawność z zapisanym w pamięci wirtualnej wzorcem. Jeżeli odciski się zgadzają, system kontroli uzyskuje pewność, że osoba korzystająca z systemu komputerowego ma do niego odpowiednie prawa. Jeżeli osoba nieupoważniona zdecyduje się przyłożyć swój palec do takowego czytnika, system po stwierdzeniu braku korelacji, blokuje dalszy dostęp do systemu.

Dzięki temu otwiera się pole do działań dla osób i grup, które próbują nieautoryzowanie, a co za tym idzie nielegalnie uzyskać dostęp do naszych danych lub naruszyć naszą prywatność. Ataki hakerskie, phishing, kradzieże tożsamości i wiele innych zagrożeń związanych z cyberprzestępczością stało się częścią naszej rzeczywistości. Dlatego też zagadnienia związane z bezpieczeństwem informacji i uwierzytelnianiem nabierają coraz większego znaczenia. Im większe grono osób nauczy się skutecznie zabezpieczać swoje dane w sieci, tym bezpieczniej mogą korzystać z dobrodziejstw internetu. Informacje o nas dostępne w wielu bazach danych są bardzo cenne dla każdego cyberprzestępcy, a zwłaszcza dla zorganizowanych organizacji, dlatego należy przykładać szczególną uwagę do sposobu ich zabezpieczania i stałego wzrostu skuteczności ochrony danych.

Techniki uwierzytelnienia można podzielić na trzy główne grupy, oparte na weryfikacji. Są to odpowiednio:

* „coś co wiesz/coś co znasz”
* „coś co masz/posiadasz”
* „coś czym jesteś”

# Cel i zakres pracy

W tej pracy skupię się na omówieniu różnych aspektów systemów uwierzytelniania, tych dostępnych dla nas od lat, oraz tych stosunkowo nowoczesnych. Analizie zostaną poddane technologie biometryczne, uwierzytelnianie dwuskładnikowe i trójskładnikowe, metody oparte na kryptografii i wiele innych. Praca zawiera również praktyczne zastosowanie uwierzytelniania wieloskładnikowego, w celu przekazania wiedzy i powagi dla skutecznego zabezpieczenia swoich danych w sieci.

Niniejsza praca ma na celu przeanalizowanie i zrozumienie kluczowych aspektów systemów uwierzytelniania oraz ich roli w ochronie dostępu do danych i usług. Celem tej pracy jest:

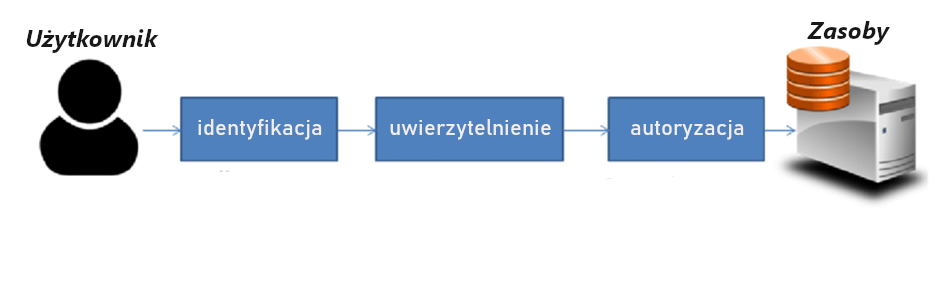
* Analiza różnych metod i technologii uwierzytelniania dostępnych na rynku.
* Zrozumienie zagrożeń i ryzyka związanego z brakiem lub słabym uwierzytelnianiem.
* Przedstawienie praktycznych przykładów wdrożeń systemów uwierzytelniania w różnych dziedzinach.

Praca składa się z pięciu rozdziałów, w których przedstawione zostaną różne aspekty uwierzytelniania użytkownika, od podstawowych pojęć, przez historię, metody i technologię uwierzytelniania, a także zagrożenia i ryzyko jakie niesie złe zabezpieczenie danych, kończąc na przyszłości uwierzytelniania.

W pracy przedstawione są również praktyczne implementacje uwierzytelniania wieloskładnikowego, co ma na celu ilustrowanie praktycznych zastosowań tej technologii oraz podkreślenie jej znaczenia dla skutecznego zabezpieczenia danych w sieci.

# Rozdział 1: Podstawy Systemów Uwierzytelniania

## Definicje i koncepcje podstawowe

Na początku trzeba zaznaczyć jakie są podstawowe różnice pomiędzy identyfikacją, uwierzytelnianiem oraz autoryzacją. Te trzy procesy będące niekiedy uznawane za tożsame i używane zamiennie w zależności od zapotrzebowania, w praktyce różnią się znacząco od siebie i posiadają inną funkcję w procesie weryfikacji.

Identyfikacja polega na jednostronnym komunikowaniu się użytkownika z systemem lub osobą odpowiedzialną (stroną ufającą) w celu przekazania swoich danych, na podstawie których dojdzie do procesu uwierzytelniania. Polega to tylko na podaniu swoich danych. Przykładem może być logowanie do konta na platformie społecznościowej, czy przekazanie swoich danych pracownikowi banku w jego placówce, w celu wykonania operacji na koncie. W pierwszym przypadku podajemy login i hasło, potrzebne do zalogowania. W drugim natomiast jest to imię, nazwisko, numer pesel, a niekiedy także numer konta bankowego. Ważne jest, że na tym etapie nie jest wymagane, by dane użytkownika były wprowadzone do bazy danych systemu, ani by były one poprawne. Tym zajmuje się uwierzytelnianie.

W kolejnym etapie weryfikacji, jakim jest uwierzytelnienie, strona ufająca, która otrzymała dane od użytkownika ma za zadanie upewnić się, czy dana osoba faktycznie podaje się za tą, do której przypisane są podane dane. Wówczas dochodzi do sprawdzenia w bazach danych, czy takie dane faktycznie są zapisane do przypisanego konta. Jeśli w bazie danych zostanie odnaleziony taki login i hasło wówczas system, który ma słaby poziom zabezpieczeń może stwierdzić, że wszystko jest w porządku i przepuści użytkownika dalej. Lepiej zabezpieczony system sprawdzi, czy taka osoba logowała się z tego konkretnego urządzenia czy też nie. Wówczas jeśli urządzenie nie jest znane w systemie dochodzi do użycia kolejnych kroków mających jednoznacznie stwierdzić, że ta osoba jest faktycznie tą, za którą się podaje. Wykorzystuje się tu uwierzytelnianie wieloetapowe (dwu lub trzy składnikowe).

Jeżeli wszystko przebiegło pomyślnie, lub też nie, wówczas dochodzi do autoryzacji. Użytkownik może zostać przepuszczony dalej, czyli uzyskać autoryzację i mieć dostęp do określonych zasobów konta, albo cofnięty do procesu identyfikacji, by cały proces rozpocząć od nowa. Przykładowo, po zalogowaniu się na serwer, czyli po poprawnej identyfikacji i uwierzytelnieniu, i uzyskaniu dostępu do zawartości serwera, użytkownik może nie mieć dostępu do określonego pliku, lub katalogu.

## Historia rozwoju systemów uwierzytelniania

Współcześnie rozumiany system uwierzytelniania znacząco ewoluował w ostatnim stuleciu przez wprowadzenie komputerów. Znacząco wcześniej takimi systemami uwierzytelniania były różnego rodzaju pieczęcie i sygnety, w celu nadania listom czy dokumentom wiarygodności. W starożytności a także w średniowieczu używano pieczęci do zabezpieczania korespondencji, a także zaświadczania autentyczności testamentu czy dokumentów. Lecz nie dotyczy to tylko dokumentów i listów. W świecie biznesowym i handlowym również musiała istnieć pewność co do kontrahentów, a system bankowy także musiał weryfikować swoich klientów i dbać o inwestycje i interesy. Przed komputerowe metody uwierzytelniania oparte były na fizycznych środkach, jak pieczęcie, sygnety, podpisy.

W miarę jak technologia komputerowa stawała się powszechna, systemy uwierzytelniania ewoluowały i dostosowywały się do nowych wyzwań i możliwości, jakie przyniosła era cyfrowa.

Wraz z rozwojem komputerów, w latach 60. XX wieku hasła stały się głównym zabezpieczeniem. W tamtych czasach niewiele osób mogło sobie pozwolić na komputer, a główną przyczyną były rozmiary takich urządzeń, ich znacząca cena. Na taki sprzęt mogły sobie pozwolić niektóre przedsiębiorstwa i uniwersytety, między innymi MIT, który wprowadził system operacyjny z podziałem czasu. Taki system umożliwił wielu użytkownikom współdzielenie zasobów. Lecz problemem stała się prywatność plików, dlatego wdrożono prosty program do obsługi haseł, a uściślając hasła były przechowywane w sposób jawny w pliku tekstowym. Dopiero na początku lat 70. XX wieku sposób przechowywania haseł uległ zmianie i zastosowano haszowanie haseł, które potem ulepszono o elementy losowe, w celu utrudnienia łamania haseł.

Do ciągłego wzrostu bezpieczeństwa haseł przyczyniło się wprowadzenie w połowie lat 70. XX wieku szyfrowania asymetrycznego. Metoda ta polega na używaniu klucza publicznego i prywatnego. Klucz publiczny może być dostępny dla każdego, natomiast klucz prywatny, który służy do weryfikacji tożsamości, musi pozostać tajnym. Do powszechnego wykorzystania tej infrastruktury doszło natomiast na początku lat 90. XX wieku.

W latach 80. XX wieku do powszechnego użytku weszły hasła jednorazowe, zmieniane po każdym logowaniu. Zwiększyło to bezpieczeństwo, gdyż po logowaniu, każda osoba mogła poznać hasło, ponieważ nie miało już ono żadnej wartości, gdyż zwyczajnie przestawało działać. Wtedy też pojawiły się problemy z generowaniem haseł, by były one losowe i nieprzewidywalne, oraz w jaki sposób dostarczać po każdym logowaniu nowe hasło użytkownikowi? Rozwiązano to dzięki osobnemu urządzeniu, które dostarczało hasło. W późniejszych latach zostanie to zastąpione SMS, e-mailem, lub aplikacjami mobilnymi.

W latach 90. XX wieku infrastruktura klucza publicznego, która była już opracowana w latach 70, została odtajniona i dostępna dla wszystkich. Wykorzystanie tego było konieczne, gdyż w sieci WWW znajdowało się pełno wrażliwych informacji i należało wiedzieć, kto ma do nich dostęp. Infrastruktura klucza publicznego obejmuje także certyfikaty cyfrowe.

W latach dwutysięcznych nastąpił rozwój uwierzytelniania wieloskładnikowego i pojedynczego logowania. Trzy główne elementy uwierzytelniania, wymagane do pomyślnej weryfikacji to wiedza (coś co użytkownik zna – hasło, pin), posiadanie (coś co użytkownik posiada – certyfikat cyfrowy, karta magnetyczna, urządzenie mobilne) oraz nieodłączność (coś czym użytkownik jest – dane biometryczne: odcisk palca, skan siatkówki oka). Pomyślne uwierzytelnianie oznacza połączenie dwóch lub więcej elementów bezpieczeństwa.

Także wówczas doszło do stworzenia logowania się w zaufaniu o stronę trzecią Single Sign-On (SSO). Polega to na logowaniu się do danej witryny za pośrednictwem konta założonego u dostawcy SSO. Użytkownik loguje się raz, a następnie może swobodnie korzystać z różnych platform, nie wpisując ponownie swoich danych uwierzytelniających. Obecnie najpopularniejsze rozwiązania to logowanie za pomocą konta Google lub konta Facebook.

Na początku drugiej dekady XXI wieku do powszechnego użytku weszło uwierzytelnianie biometryczne. Wykorzystanie odcisku palca, rozpoznawania twarzy, skanu tęczówki oka zaczęło być bardzo popularne wraz ze wzrostem popularności smartfonów i innych urządzeń mobilnych. Pierwszym smartfonem wykorzystującym odcisk palca była Motorola ATRIX z systemem android. W 2017 roku firma Apple stworzyła Face ID, które za pomocą podczerwieni skanuje twarz użytkownika. Obecnie biometria jest częścią naszej rutyny – odblokowywania naszych smartfonów, potwierdzania zakupów online itp. Są niezwykle trudne do sfałszowania i uważane są za jedną z najbezpieczniejszych dostępnych metod uwierzytelniania.

## Znaczenie i rola systemów uwierzytelniania w bezpieczeństwie informatycznym

Systemy uwierzytelniania pełną ważną rolę w zapewnieniu bezpieczeństwa informatycznego naszym danym, umieszczonym w różnych bazach danych różnych firm, organizacji, a także organom państwowym. Kluczowe jest skuteczne i mocne zabezpieczenie wszystkich wrażliwych danych mogących – w niepowołanych rękach – uczynić wiele szkód i strat. Uwierzytelnianie zapewnia wiele mechanizmów potwierdzania tożsamości użytkownika i kontroli dostępu do systemów, danych oraz zasobów.

Nasza zależność od komputerów, urządzeń mobilnych i internetu stale rośnie, co niesie za sobą ogromne korzyści, ale również narasta ryzyko związanego z utratą prywatności, kradzieżą tożsamości i innymi zagrożeniami związanymi z bezpieczeństwem informatycznym. W tym kontekście systemy uwierzytelniania, które odpowiadają za weryfikację tożsamości użytkowników oraz kontrolę dostępu do zasobów, stają się nieodłącznym elementem ochrony przed potencjalnymi zagrożeniami.

Słabe uwierzytelnianie lub jego brak może prowadzić do różnego rodzaju ataków oraz naruszeń. Doprowadza to w głównej mierze do udzielenia dostępu do systemów, aplikacji, danych i zasobów (także materialnych) osobom niepowołanym, co może skutkować do poważnych skutków takich jak kradzież wrażliwych danych, niszczenie informacji lub nieautoryzowanego korzystania z różnych kont. Przykładowo nikt nie chciałby, by ktoś mógł w bardzo prosty sposób dostać się do zasobów naszego konta bankowego i wypłacać z niego środki do woli, czy też przeglądać nasze prywatne zdjęcia, filmy, czy coś bardzo prywatnego zapisanego na dysku komputera. Chcemy te pliki, dane i dostęp zachować tylko dla siebie, by nikt poza nami nie mógł mieć dostępu do naszych informacji. Dlatego ważne jest silnie zabezpieczać swoje dane.

Korzyści z wdrożenia bezpiecznego uwierzytelniania w bezpieczeństwie aplikacji są liczne. Po pierwsze, minimalizuje ryzyko nieuprawnionego dostępu, chroniąc wrażliwe dane użytkowników i cenne zasoby przed złośliwymi podmiotami. Weryfikując tożsamość użytkowników, zmniejsza prawdopodobieństwo przejęcia konta lub podszywania się, zwiększając zaufanie i zaufanie użytkowników do aplikacji.

Słabe zabezpieczenie tylko motywuje hakerów do atakowania i wykradania cennych danych z kont prywatnych ale także – o wiele cenniejszych – kont firmowych, w celu zdobycia wszystkich danych o użytkownikach i wykorzystaniu ich dla swoich potrzeb. Stosując słabe hasła z łatwością – poprzez wykonanie ataków „brute-force” można uzyskać hasło do konta i korzystać z niego bez ograniczeń.

Dla firm, które stosują słabe uwierzytelnianie swoich produktów, ale także swoich firmowych systemów, w przypadku udanego ataku może skutkować utratą reputacji, a co za tym idzie doprowadzić do upadku firmy. Klienci stwierdzą, że firma ta nie zapewnia bezpieczeństwa ich danych i zamiast zakupić ich produkt czy usługę, skierują się do konkurencji. Takie zachowania w dłuższym etapie czasu może zwyczajnie doprowadzić do kłopotów finansowych firmy, a nawet jej upadku.

Współcześnie niestosowanie zabezpieczeń, lub używanie ich w stopniu niewystarczającym dla współczesnych standardów może doprowadzić w przypadku ataku do naruszenia regulacji i przepisów prawnych. Wówczas może dojść do wymierzenia przez organy ścigania odpowiednich kar finansowych.

Biometria znacząco przyczynia się do wzrostu siły zabezpieczeń, a co za tym idzie znacząco utrudnia potencjalnemu hakerowi dostęp do naszych danych, pieniędzy czy kont. Ocena wielu cech biologicznych w celu identyfikacji tożsamości jednostki może znacznie usprawnić działanie systemu.

Jednym z najważniejszych elementów, które należy wziąć pod uwagę w nowoczesnych systemach uwierzytelniania, jest kompromis między użytecznością a bezpieczeństwem. Podejście uwierzytelniania wieloskładnikowego pozwala na zastosowanie szerokiego zakresu sytuacji, w których bezpieczeństwo jest najważniejsze.

# Rozdział 2: Klasyczne Metody Uwierzytelniania

## Uwierzytelnianie oparte na czymś, co się wie (wiedza)

Uwierzytelnianie oparte na wiedzy to wszelkiego typu hasła, kody PIN, kody jednorazowe, pytania bezpieczeństwa, certyfikaty i klucze prywatne. W każdym sposobie uwierzytelniania jest możliwe wykradzenie informacji i wykorzystaniu jej przeciwko właścicielowi danych czy konta.

Uwierzytelnianie oparte na wiedzy i informacjach samo w sobie nie jest wystarczająco skutecznym zabezpieczeniem. Klasyczne metody uwierzytelniania, takie jak hasło czy kod PIN, są jednym z najstarszych i wciąż jednymi z najpopularniejszych metod potwierdzania naszej tożsamości. Uwierzytelnianie w najprostszej formie polega na podaniu loginu i hasła. Zastosowanie tylko jednego składnika podczas logowania jest w dzisiejszych czasach niewystarczalne, dlatego nie jest dobrą metodą opierać się wyłącznie na tym sposobie uwierzytelniania. Bezpieczeństwo stosowania loginu i hasła, czy też samego kodu PIN jest wysoce nieodpowiedzialne i niebezpieczne.

Największe wady stosowania haseł:

* Hasło można odgadnąć za pomocą prób i błędów, lub stosując odpowiednie oprogramowanie za pomocą na przykład metody wyszukiwania wyczerpującego brute-force, albo poprzez metodę słownikową.
* Jeżeli hasło jest przesyłane w sposób źle zabezpieczony, lub co gorsza w sposób jawny, takie hasło można podsłuchać podczas transmisji a następnie odszyfrować i wykorzystać.
* Wymyślanie nowych haseł i posiadanie ich sporo w swojej głowie powoduje, że z czasem można zapomnieć hasła do logowania, co prowadzi do utraty dostępu do konta. Jeżeli użytkownik zapomni hasła do platformy społecznościowej i nie pamięta hasła do skrzynki pocztowej, może dojść do sytuacji utraty konta, gdyż odzyskanie dostępu może być utrudnione.
* Hasła się starzeją i czas potrzebny na ich złamanie również, dlatego trzeba je często zmieniać i zadbać o to by były skomplikowane.
* Użytkownicy powinni być ostrożni wobec prób phishingu, czyli prób oszustwa polegających na przekonaniu ich do podania swoich haseł. Ważne jest, aby weryfikować strony internetowe i źródła, z których pochodzą żądania podania hasła.

Tworzenie haseł to ważna czynność i dlatego użytkownik powinien przemyśleć, czy zastosowanie danego hasła przełoży się na większe bezpieczeństwo swojego konta. Powinno stosować się do reguł, które mają na celu zwiększenie siły hasła:

* Hasło powinno być dłuższe niż 8-10 znaków, im dłuższe hasło tym lepiej.
* Powinno składać się z małych, dużych liter, a także z liczb i znaków specjalnych.
* Hasło nie może być takie same jak login, ani jak twoje imię czy nazwisko.
* Można stosować zamianę liter na znaki specjalne: zamiast litery „a” można użyć „@”, analogicznie litera „i” lub „l” na „!”, literę „s” na „$”. Lub losowo np.: „H” na „\*”. Choć obecnie nie jest to dużym problemem dla hakerów.
* Jedno hasło do jednego konta. Nie używaj tego samego hasła do kilku kont stosując lekką modyfikację oryginału.

Poniżej znajduje się przykładowy kod, który implementuje atak Brute Force w celu złamania hasła. Po wpisaniu hasła, które ma ulec złamaniu, program za pomocą pętli, generuje wszystkie możliwe kombinacje znaków o zmiennych długościach, zaczynając od pojedynczych znaków i zwiększając długość do długości hasła docelowego. Każda wygenerowana kombinacja jest konwertowana na string, a następnie porównywana z hasłem docelowym. Jeśli zostanie znalezione dopasowanie, funkcja zwraca krotkę zawierającą liczbę prób i odgadnięte hasło.

1. import itertools

2. import string

3.

4. def atak\_bruteforce(haslo\_docelowe):

5. znaki = string.printable.strip()

6. laczna\_liczba\_prob = 0

7.

8. for dlugosc in range(1, len(haslo\_docelowe) + 1):

9. for krotka\_prob in itertools.product(znaki, repeat=dlugosc):

10. laczna\_liczba\_prob += 1

11. aktualna\_probka = ''.join(krotka\_prob)

12. if aktualna\_probka == haslo\_docelowe:

13. return (laczna\_liczba\_prob, aktualna\_probka)

14.

15. return (laczna\_liczba\_prob, None)

16.

17. haslo\_docelowe = input("Podaj hasło do złamania: ")

18. ilosc\_prob, zgadniete\_haslo = atak\_bruteforce(haslo\_docelowe)

19.

20. if zgadniete\_haslo:

21. print(f"Hasło zostało złamane po {ilosc\_prob} próbach. Hasło to {zgadniete\_haslo}.")

22. else:

23. print(f"Hasło nie zostało złamane po {ilosc\_prob} próbach.")

24.

Metoda ta ma dużą złożoność obliczeniową, co dla bardzo długich kluczy sprawia, że złamanie klucza jest praktycznie niemożliwe. Natomiast dla krótkich i prostych haseł ten sposób spełni swoje zadanie. Jednakże współczesne systemy logowania posiadają limity błędnych prób logowania, co znacznie wydłuża czas działania algorytmu, a także skutecznie blokuje dostęp do konta.

W aplikacji „Be Safe Warrior”, która jest częścią tej pracy, znajduje się narzędzie do sprawdzania siły hasła i jednocześnie zwraca użytkownikowi sugestie wzmacniające hasło oraz to, jakimi metodami może dojść do złamania hasła. Strona korzysta z narzędzia zxcvbn, które szacuje siłę hasła na podstawie wzorców.

Bruteforce - Technika próbująca złamać hasło poprzez iteracyjne przetestowanie wszystkich możliwych kombinacji. Algorytm ten ocenia siłę hasła, uwzględniając odporność na ataki brute-force.

Date (data): obejmuje sprawdzanie, czy hasło zawiera daty, co może zwiększać jego przewidywalność. Algorytm ten może uwzględniać daty jako potencjalne słabe punkty w haśle.

1. var \_const = require('../../data/const.js');

2.

3. var dateMatcher = (({

4. year,

5. separator

6. }) => {

7. // base guesses: (year distance from REFERENCE\_YEAR) \* num\_days \* num\_years

8. const yearSpace = Math.max(Math.abs(year - \_const.REFERENCE\_YEAR), \_const.MIN\_YEAR\_SPACE);

9. let guesses = yearSpace \* 365;

10. // add factor of 4 for separator selection (one of ~4 choices)

11. if (separator) {

12. guesses \*= 4;

13. }

14. return guesses;

15. });

16.

17. module.exports = dateMatcher;

18.

Wewnątrz funkcji obliczane są wartości związane z odgadywaniem hasła. Najpierw obliczane jest odległość między podanym rokiem a stałą \_const.REFERENCE\_YEAR - to jest rok odniesienia, a następnie używana jest funkcja Math.max, aby uzyskać większą wartość spośród bezwzględnych różnic. Obliczana jest również wartość guesses na podstawie przestrzeni lat i liczby dni w roku.

Dictionary (słownik): algorytm korzysta z list słów (słownika) do oceny siły haseł. Jeżeli hasło można znaleźć w słowniku, może być uznane za słabe. Im bardziej rozbudowany słownik tym lepiej.

Regex (wyrażenie regularne): Algorytm korzysta z wyrażeń regularnych do identyfikowania określonych wzorców w haśle, co pozwala na ocenę jego siły.

Repeat (powtarzanie): Algorytm sprawdza, czy hasło zawiera powtarzające się sekwencje znaków, co może wpływać na jego ocenę.

Separator (separator): uwzględnia używanie separatorów lub innych specjalnych znaków do zwiększenia różnorodności i złożoności hasła.

Sequence (sekwencja): Algorytm analizuje, czy hasło zawiera proste sekwencje znaków, takie jak "abc" lub "123", co wpływa na ocenę jego siły.

Spatial (przestrzeń): słowo kluczowe może sugerować analizę klawiatury lub układu znaków w haśle, aby wykrywać potencjalne wzorce. Przykładowo ciąg "qwerty" znajduje się obok siebie na klawiaturze, co ułatwia odgadnięcie ciągu hasła.

Zxcvn wykorzystuje różne techniki, takie jak analiza dat, sprawdzanie słowników, wyrażeń regularnych, powtarzających się sekwencji, separatorów, sekwencji znaków oraz przestrzennych aspektów hasła, aby dokładnie ocenić jego siłę i przeciwdziałać atakom.

W dzisiejszych czasach każdy z nas posiada konta na różnych stronach internetowych, zaczynając od serwisów społecznościowych, serwisy streamingowe, internetowe konta bankowe, konto w Urzędzie Skarbowym czy Zakładzie Ubezpieczeń Społecznych. Duża ilość kont, do których należy mieć różne loginy i długie, bezpieczne, skomplikowane hasła. Nie można używać tych samych haseł do kilku kont, więc pojawia się problem z zapamiętaniem tego wszystkiego. Zapisanie wszystkich takich danych na kartce papieru i noszenie przy sobie jest bardzo niebezpieczne z kilku powodów: taką kartkę można zgubić, ktoś może podejrzeć jej zawartość, a w przypadku zniszczenia jej przez zalanie tracimy możliwości do dostępu do swoich kont, a ich odzyskanie może być wyjątkowo trudne, lub wręcz niemożliwe.

Z pomocą w takiej sytuacji przychodzą różnego rodzaju menadżerzy haseł, które w bezpieczny, szyfrowany sposób zapisują je wszystkie, a nawet generują losowe hasła co pewien czas, by konta były na pewno zabezpieczone. Lecz trzeba tu nadmienić, że do takiego menadżera też trzeba znać hasło. W innym wypadku wszystkie zapisane hasła, loginy, adresy e-mail zostaną utracone. Dobrą praktyką jest znać tylko dwa hasła: jedno do menadżera haseł, drugie do swojej skrzynki mailowej. Gdy stracimy dostęp do menadżera haseł, wówczas wszystkie linki do odzyskania kont przyjdą właśnie na skrzynkę mailową.

Największe wady stosowania kodów PIN:

* PIN-y składają się z cyfr, co ułatwia złamanie kodu za pomocą brute force, w których atakujący próbują wszystkie możliwe kombinacje, aby odgadnąć PIN.
* Zazwyczaj składają się z 4 lub 6 cyfr. Dzięki temu są stosunkowo łatwe do zapamiętania przez osoby „podglądające”.
* Brak różnorodności w znakach, co ogranicza różnorodność. W przeciwieństwie do haseł, PIN-y nie zawierają liter ani znaków specjalnych.

W wielu przypadkach, organizacje i dostawcy usług wprowadzają dodatkowe zabezpieczenia w celu zwiększenia bezpieczeństwa PIN-ów, takie jak mechanizmy blokady po wielokrotnych próbach wprowadzenia, dwuskładnikowe uwierzytelnianie. Jednak nadal istnieją pewne ograniczenia i zagrożenia związane z PIN-ami, dlatego ważne jest, aby stosować je z rozwagą i ostrożnością oraz rozważać inne metody uwierzytelniania tam, gdzie to możliwe.

## Uwierzytelnianie oparte na czymś, co się ma (posiadanie)

Uwierzytelnianie oparte na czymś, co się ma, to metoda uwierzytelniania, która polega na potwierdzaniu tożsamości użytkownika na podstawie fizycznego przedmiotu lub czegoś, co użytkownik posiada. Ta forma uwierzytelniania ma na celu zabezpieczenie dostępu do systemów, kont, lub zasobów poprzez wykorzystanie czegoś, co jest fizycznie obecne lub w posiadaniu użytkownika. Obejmuje to różne rodzaje fizycznych nośników, które służą do potwierdzania tożsamości, takie jak karty identyfikacyjne, karty magnetyczne, tokeny, czy klucze ale także uwierzytelnianie w aplikacji na naszym smartfonie.

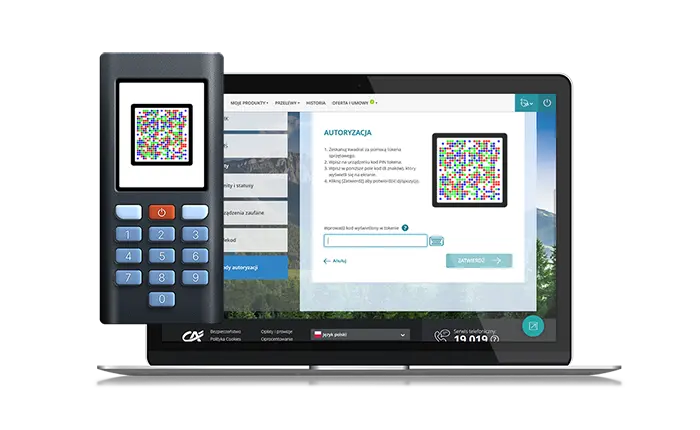
Stosowanie tego typu uwierzytelniania nie odnosi się wyłącznie do strefy wirtualnej, podczas logowania na konta, czy do systemu. Bardzo często wykorzystuje się uwierzytelnianie oparte na czymś co posiadamy w codziennym życiu, między innymi w pracy, na uczelni, czy wielu innych miejscach.

Karty identyfikacyjne są powszechnym przykładem tego typu uwierzytelniania. Są to fizyczne karty, na których znajdują się informacje identyfikacyjne, takie jak imię, nazwisko, zdjęcie, numer identyfikacyjny, data ważności, oraz np. kod kreskowy. Użytkownik musi posiadać tę kartę i za każdym razem przyłożyć ją do czytnika w celu uzyskania dostępu do budynku, pomieszczenia lub systemu, lub w celu zaznaczenia w systemie początku oraz końca pracy. Niekiedy wejście na teren firmy bez takiej karty jest niemożliwe i wówczas trzeba udowodnić np.: pracownikowi ochrony, że faktycznie jest się pracownikiem firmy oraz wypełnić odpowiedni dokument. Karta identyfikacyjna może zawierać pasek magnetyczny albo chip, wykorzystujący technologię RFID lub NFC.

Karta magnetyczna to rodzaj plastikowej karty wyposażonej w pasek magnetyczny, na którym zapisane są dane identyfikacyjne lub kody dostępu. Karty magnetyczne są powszechnie stosowane do różnych celów, takich jak kontrole dostępu, płatności, identyfikacja pracowników, karty biblioteczne, dowody osobiste, bilety komunikacji miejskiej, w niektórych krajach także prawo jazdy zawiera pasek magnetyczny.

W systemie bankowym stosuje się karty elektroniczne, które zawierają mikroprocesor dla płatności zbliżeniowych, często też posiadają paski magnetyczne. Są one bardziej zaawansowane niż tradycyjne karty magnetyczne, są bezpieczniejsze i zawierają wiele funkcjonalności. Mikroprocesor na karcie może obsługiwać protokoły kryptograficzne, co pozwala na zabezpieczenie przechowywanych danych i transakcji. Są bardziej odporne na kradzieże danych lub podszywanie się pod innych użytkowników.

Kolejnym przedmiotem używanym w uwierzytelnianiu sprzętowym są klucze sprzętowe. Fizyczne klucze uwierzytelniające to obecnie jedne z najskuteczniejszych metod ochrony przed przejmowaniem kont i phishingiem. Klucze fizyczne są zazwyczaj małymi urządzeniami elektronicznymi, które użytkownik musi posiadać fizycznie, aby uzyskać dostęp. Uwierzytelnianie sprzętowe jest bardzo bezpieczne, ponieważ musisz fizycznie posiadać klucz i go przedstawić. Oznacza to, że phisher działający w internecie nie może po prostu nakłonić kogoś do przekazania hasła lub nawet hasła wraz z kodem drugiego składnika w celu włamania się na konto cyfrowe. Klucze są zazwyczaj wyposażone w zaawansowane mechanizmy kryptograficzne, które służą do zabezpieczania przechowywanych na nich danych. Takie urządzenie może zawierać prywatny klucz kryptograficzny, który jest używany do podpisywania lub deszyfrowania danych. Dzięki temu nawet jeśli klucz zostanie skradziony, dane pozostają bezpieczne.

Tokeny są kolejnym sposobem zabezpieczania swoich danych. Jest to nic innego jak niewielkie urządzenie peryferyjne, na którym wyświetlany jest kod w formie ciągu znaków, który należy przepisać np. do systemu bankowego w celu zatwierdzenia przelewu. Niektóre systemy bankowe korzystają z technologii Cronto, która podczas płatności generuje na ekranie komputera grafikę podobną do kodu QR, który za pomocą tokenu należy zeskanować, a następnie urządzenie poprosi o podanie kodu PIN.

# Rozdział 3: Nowoczesne Technologie Uwierzytelniania

Nowoczesne metody uwierzytelniania przekraczają tradycyjne podejście opierające się na zapamiętywaniu haseł lub korzystaniu z PIN-ów, ani na posiadaniu fizycznych przedmiotów, czy urządzeń. W tej metodzie to sam człowiek jest wystarczający do uwierzytelnienia się, w zależności od tego, jaką technologię wybierze do tego celu.

Uwierzytelnianie na podstawie tego czym się jest, ułatwia w dużym stopniu skomplikowanie uwierzytelniania się, a przy tym jednocześnie nie dochodzi do spadku stopnia zabezpieczeń. Jest to spowodowane tym, że wszystko co jest do tego potrzebne to osoba, która ma zostać poddana weryfikacji. Dzięki temu rozwiązaniu nie ma konieczności zapamiętywania długich i trudnych haseł, które często są źródłem frustracji i stanowią potencjalne zagrożenie, jeśli zostaną przechwycone lub odgadnięte.

Jest to jedna z najnowocześniejszych i najbardziej zaawansowanych form uwierzytelniania, która opiera się na fizycznych lub behawioralnych cechach, które są unikalne dla każdej osoby. W tym celu używa się metod biometrycznych, takich jak odcisk palca, skan twarzy, skan siatkówki oka, czy sprawdzenie brzmienia głosu.

Nowoczesne technologie uwierzytelniania nie są oparte wyłącznie na osobie. Ponieważ poza biometrią istnieją takie aspekty jak: ciągłe uwierzytelnianie, czy uwierzytelnianie adaptacyjne. Podczas korzystania z płatności internetowych nie raz zdarzyło się tak, że przeskakując ze strony na stronę nagle zostaliśmy wylogowani i poproszeni o ponowne zalogowanie. Jest to spowodowane tym, że ciągłe uwierzytelnianie cały czas „patrzy nam na ręce” i kontroluje nasze działania podczas korzystania z konta. Mechanizmy ryzyka muszą analizować szeroki zakres danych o użytkowniku, nawet częstotliwość wpisywanych znaków na klawiaturze, aby zweryfikować jego tożsamość w czasie rzeczywistym. Silnik ryzyka wykorzystuje kilka czynników do analiz, ustalając, czy konkretna sesja użytkownika stwarza podwyższone ryzyko.

## Uwierzytelnianie biometryczne

Jednym z powszechnie stosowanych rodzajów uwierzytelniania opartego na biometrii jest rozpoznawanie odcisku palca. Obecnie znaczna większość urządzeń mobilnych posiada skaner linii papilarnych i to uwierzytelnianie jest stosowane jako jedne z podstawowych. Użytkownik po prostu umieszcza swój palec na czytniku, a system dokładnie analizuje odczytany unikalny wzór linii papilarnych, z tym zapisanym w pamięci urządzenia. Technologia ta w przeszłości była niebezpieczna, ponieważ zastosowanie słabej jakości czytnika, powodowało, że można go było stosunkowo łatwo oszukać. Współcześnie systemy uwierzytelniania biometrycznego są mniej narażone na ataki ze strony hakerów, ponieważ uzyskanie zwykłego hasła jest znacznie prostsze od podrobienia unikalnej fizycznej cechy danego człowieka. Technologia wciąż się rozwija, co skutkuje tym, że jest coraz bardziej odporna na próby oszustwa.

Rozwinięciem tej metody jest geometria dłoni, która mierzy kształt, formę, czy wymiary dłoni, które są monitorowane i mierzone przez biometryczny system rozpoznawania dłoni. W różnych obszarach dłoni można znaleźć zróżnicowane szerokości i grubości palców oraz stawów. Przy obliczaniu geometrii dłoni brane są pod uwagę różne aspekty naskórka dłoni, takie jak fałdy i linie. Obraz dłoni jest rejestrowany przy użyciu płaskiego skanera o otwartej powierzchni, co wyeliminowało potrzebę umieszczania dłoni osoby w jednej pozycji. Niektóre dzisiejsze systemy wykorzystują standardowe kamery, które nie wymagają bliskiego kontaktu z powierzchnią rejestrującą.

Inną metodą jest skan twarzy, gdzie aparat kamery zbiera dane o strukturze twarzy i porównuje je z zapisanym wzorcem. Porównywane są takie elementy jak: odległość między oczami, szerokość nosa, odległości kości policzkowych i innych unikalnych cech użytkownika. Skany twarzy na początku istnienia w np.: urządzeniach mobilnych polegały na analizie obrazów punktów orientacyjnych, które można było ominąć, pokazując zdjęcie twarzy wydrukowane na papierze. Technologia rozwinęła się i za pomocą trójwymiarowego rozpoznawania twarzy może zidentyfikować rzeczywiste miny użytkownika.

Skan oczu jest jedną z metod identyfikacji użytkownika, który wykonuje zdjęcie tęczówki oka. Lecz zanim dojdzie do wykonania takiego zdjęcia potrzebna jest kamera bardzo wysokiej rozdzielczości, która wykorzystuje także podczerwień do oświetlania tęczówki. Następnie dochodzi do szczegółowej analizy, podczas której sprawdzane są takie parametry jak: kształt, kontur tęczówki, czy wykrycie położenia źrenicy. Dodatkowo analiza siatkówki oka pozwala na wychwycenie i przeanalizowanie naczyń krwionośnych w tylnej części oka. Skan siatkówki oka jest jednym z najbardziej wydajnych i niezawodnych sposobów uwierzytelniania, lecz wymaga posiadania drogiego sprzętu.

Powyższe metody uwierzytelniania biometrycznego są najpopularniejszymi w codziennym użytkowaniu, lecz poza nimi jest jeszcze szereg innych metod, o wiele bardziej skomplikowanych i bardziej specjalistycznych niż do codziennego uwierzytelniania.

Czujniki termiczne są wykorzystywane do generowania unikalnego obrazu cieplnego struktury naczyń krwionośnych twarzy konkretnej osoby. Jest to szczególnie przydatne w przypadkach, gdy występuje niedostateczne oświetlenie. Jednakże samopoczucie osoby badanej i jej stan zdrowotny ma znaczenie podczas mierzenia, a co za tym idzie może mieć wpływ na zebrane dane podczas takiego skanu.

Wpływ położenia geograficznego na system uwierzytelniania może nie koniecznie być dobrą metodą, ponieważ we współczesnym świecie bardzo często podróżujemy i zmieniamy miejsca swojego pobytu. Logowanie do konta bankowego czy do serwisu społecznościowego tylko z wcześniej określonej lokalizacji stanowiłby znaczne utrudnienie. Lecz jest często wykorzystywane w serwisach streamingowych, gdzie dostęp do danego filmu, serialu, czy wydarzenia sportowego może być zablokowany. Do listy dozwolonych lub blokowanych można dodać określoną lokalizację geograficzną, niezależnie od poziomu dostępu danej osoby.

Jednowymiarowe sygnały biomedyczne, takie jak elektrokardiogram (EKG), można wykorzystać jako charakterystykę biometryczną. Zapisy EKG ujawniają informacje na temat transmisji elektrycznej w sercu i służą do identyfikacji konkretnych użytkowników. EKG jest silnie powiązane z indywidualnymi cechami serca każdej osoby. Powszechnie wiadomo, że serce każdego człowieka ma odrębne cechy fizjologiczne ze względu na różnice genetyczne. Takie drobne różnice wpływają na pracę serca i mogą być widoczne w EKG każdego użytkownika. Niekontrolowane warunki pobierania mogą znacząco obniżyć skuteczność urządzeń biometrycznych EKG.

Kod genetyczny każdego człowieka – tak samo jak odcisk palca – jest unikalny i może posłużyć do uwierzytelniania osoby. Proces gromadzenia i analizowania danych jest czasochłonny i kosztowny, lecz jest możliwy do uwierzytelniania użytkownika w wysoce tajnego obiektu lub do wrażliwych, ściśle tajnych informacji lub danych.

## Uwierzytelnianie wieloskładnikowe (MFA)

Uwierzytelnianie wieloskładnikowe jest jedną z metod zabezpieczania dostępu do systemów, kont użytkowników czy danych poprzez wykorzystanie co najmniej dwóch różnych czynników uwierzytelniania. W ten sposób można bardziej zabezpieczyć nasze dane czy konta, ponieważ bezpieczeństwo nie opiera się wyłącznie na jednym składniku, lecz na co najmniej dwóch, a co za tym idzie szanse, by osoba podszywająca się pod nas miała uzyskać dostęp są coraz niższe, w zależności od wzrostu stopnia zabezpieczeń.

Każdy ze składników powinien być unikalny i trudny do odgadnięcia przez osoby trzecie. Oznacza to, że jeśli w uwierzytelnianiu wieloskładnikowym stosujemy na przykład login i hasło, a do tego potwierdzenie odciskiem palca w aplikacji mobilnej, to samo hasło powinno spełniać wszystkie wymagania, by było silnym – odpowiednio długim i skomplikowanym. Zwiększa ono trudność dla potencjalnych atakujących, ponieważ nawet w przypadku przechwycenia jednego z czynników, dostęp do systemu nie jest możliwy bez drugiego czynnika uwierzytelniającego.



Stosowanie uwierzytelniania dwuskładnikowego może przyczynić się do wzrostu bezpieczeństwa, a stosowanie trzech składników jeszcze mocniej utrudni potencjalne włamania na konta. Lecz musimy być uważni, by nie podawać naszych danych na stronach podszywających się pod te, na których mamy konta, bo najzwyczajniej w świecie nieświadomie podajemy swoje dane wprost hackerowi. Niestety wiele składników przyczynia się do trudniejszego dostępu także dla nas, ponieważ podczas logowania poza podaniem loginu i hasła, musimy także zalogować się na pocztę i sprawdzić wiadomość mail z kodem uwierzytelniającym, by następnie podać go na stronie logowania.

## Uwierzytelnianie oparte na kryptografii

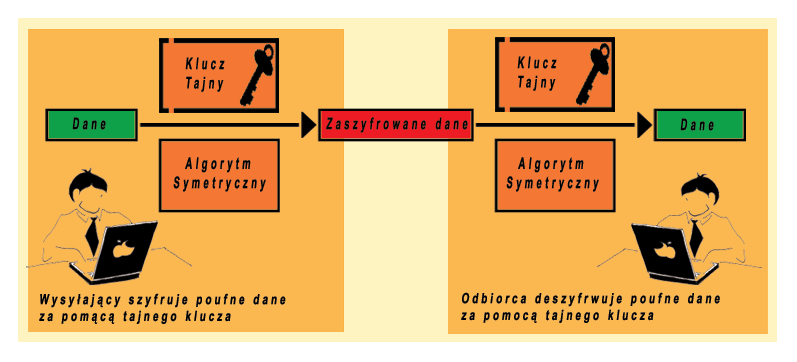
Uwierzytelnianie kryptograficzne (oparte na kluczach) pozwala stronom ufającym mieć pewność, że dane podawane przez użytkowników są rzeczywiście prawdziwe, poprzez wykorzystanie kryptografii. Taki rodzaj uwierzytelniania jest alternatywny do stosowania haseł, ponieważ zamiast podać login i hasło, wystarczy, że prześle się odpowiedni klucz.

Uwierzytelnianie tego typu można podzielić na dwa sposoby: uwierzytelnianie symetryczne i asymetryczne.

Uwierzytelnianie symetryczne to rodzaj uwierzytelniania, w którym zarówno strona wysyłająca – użytkownik, jak i strona odbierająca – serwer, używają wspólnego klucza (klucza symetrycznego) do uwierzytelnienia siebie nawzajem. Klucz ten jest tajny i znany tylko obu stronom, co oznacza, że obie strony muszą znać ten sam sekretny klucz, aby się uwierzytelnić. Tego typu uwierzytelnianie jest dość proste i efektywne, ale także ma swoje ograniczenia. Głównym zagrożeniem jest to, że obie strony muszą w sposób bezpieczny przechowywać sekretny klucz. W przypadkach, gdzie wymagana jest większa odporność na ataki, takie jak dostęp zdalny do systemów lub usług internetowych, często stosuje się uwierzytelnianie asymetryczne, które oferuje wyższy poziom bezpieczeństwa.

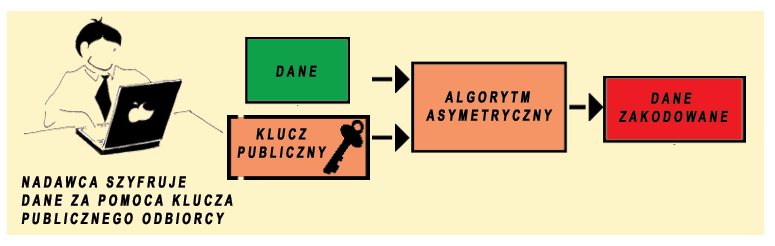
Proces uwierzytelniania symetrycznego może wyglądać następująco:

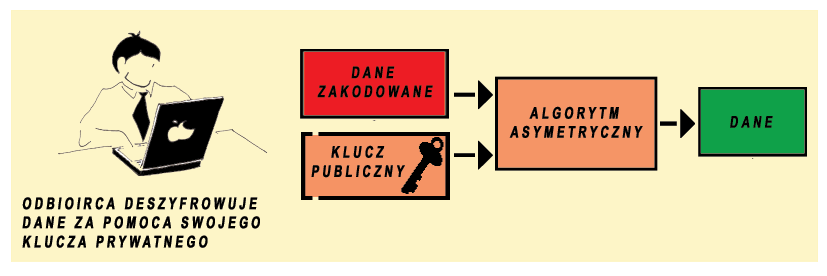
* Strona wysyłająca i strona odbierająca mają wspólny sekretny klucz.
* Strona wysyłająca wysyła do strony odbierającej wiadomość uwierzytelniającą, która jest zabezpieczona za pomocą tego wspólnego klucza.
* Strona odbierająca odbiera wiadomość i próbuje odkodować ją przy użyciu tego samego klucza.
* Jeśli odkodowanie wiadomości jest sukcesem, to strona odbierająca jest w stanie zweryfikować tożsamość strony wysyłającej i uwierzytelnia ją.



Uwierzytelnianie asymetryczne to proces uwierzytelniania, w którym wykorzystywane są pary kluczy kryptograficznych, składające się z klucza publicznego i klucza prywatnego. Klucz publiczny jest dostępny publicznie i może być udostępniany na szeroką skalę, podczas gdy klucz prywatny jest przechowywany tajnie i znany jedynie właścicielowi. Klucz publiczny jest używany do weryfikacji podpisów cyfrowych i szyfrowania wiadomości, podczas gdy klucz prywatny służy do tworzenia podpisów cyfrowych i deszyfrowania wiadomości. Dzięki temu procesowi uwierzytelniania możliwa jest potwierdzanie tożsamości w sposób, który jest trudny do sfałszowania. Klucz prywatny jest tajny i trudny do złamania, co zapewnia wysoki poziom bezpieczeństwa. Podczas komunikacji klucze publiczne mogą być wymienianie w sposób bezpieczny, bo nawet ich wykradzenie nie spowoduje utraty danych.

* Użytkownik generuje parę kluczy asymetrycznych - klucz publiczny i klucz prywatny. Klucz publiczny jest przekazywany publicznie, a klucz prywatny jest ściśle chroniony.
* Klucz publiczny jest przekazywany lub rejestrowany w systemie lub na serwerze, z którym użytkownik chce się uwierzytelnić.
* Użytkownik wysyła prośbę o uwierzytelnienie do strony lub serwera, często z dołączonymi danymi uwierzytelniającymi, takimi jak podpis cyfrowy wygenerowany przy użyciu klucza prywatnego.
* Strona lub serwer odbierający prośbę sprawdza klucz publiczny użytkownika, aby upewnić się, że jest zgodny z przekazanym wcześniej kluczem publicznym.
* Jeśli użytkownik dołączył podpis cyfrowy, strona lub serwer weryfikuje go przy użyciu klucza publicznego użytkownika.
* Jeśli wszystkie weryfikacje są pomyślne, strona lub serwer uwierzytelnia użytkownika.





Jednym z najpopularniejszych, a zarazem pierwszych algorytmów asymetrycznych był RSA. Został on zaprojektowany w 1977 roku. Klucz ma zwykle od 1000 do 4000 bitów. RSA jest generalnie uważany za bezpieczny system zabezpieczeń i jest powszechnie stosowany w przeróżnych aplikacjach, protokołach i rodzajach komunikacji.

# Rozdział 4: Zagrożenia i Ryzyko w Systemach Uwierzytelniania

Systemy uwierzytelniania stanowią pierwszą linię obrony przed nieautoryzowanym dostępem do danych, aplikacji i zasobów. Niemniej jednak, te systemy nie są odporne na zagrożenia, a ich niewłaściwe zarządzanie niesie ze sobą znaczne ryzyko. Zagrożenia i ryzyko związane z systemami uwierzytelniania są poważnym wyzwaniem dla dziedziny bezpieczeństwa informatycznego.

Łamanie szyfrów to jedno z głównych zagrożeń w kontekście systemów uwierzytelniania. Szyfry są stosowane w celu zabezpieczenia danych, w tym haseł i informacji uwierzytelniających, co czyni je atrakcyjnym celem dla atakujących. Poniżej omówimy, jak łamanie szyfrów może stanowić zagrożenie dla systemów uwierzytelniania.

Hasła użytkowników są zazwyczaj przechowywane w zaszyfrowanej formie. To oznacza, że oryginalne hasła są transformowane za pomocą matematycznych operacji lub algorytmów kryptograficznych w nieczytelny dla ludzi zapis. Taki proces pozwala na zabezpieczenie danych użytkowników przed dostępem nieautoryzowanym.

Jednak atakujący mogą próbować złamać te szyfry, aby uzyskać dostęp do haseł lub informacji uwierzytelniających.

## Ataki na systemy uwierzytelniania

Ataki na systemy uwierzytelniania to różnorodne techniki, których celem jest obejście lub złamanie mechanizmów uwierzytelniania, co umożliwia dostęp nieautoryzowanym osobom do systemów, kont użytkowników lub danych. Zadanie to jest uproszczone, gdy użytkownik stosuje zbyt słabe zabezpieczenia, to znaczy używa tylko loginu i hasła, a hasło samo w sobie jest słabe. A uzyskanie dostępu jest jeszcze o tyle prostsze, jeżeli użytkownik używa jednego hasła na różnych stronach.

Metody ataków wykorzystujące inżynierię społeczną (nazywaną również socjotechniką) opierają się głównie na wykorzystaniu mechanizmów psychologicznych w celu uzyskania poufnych informacji. Cyberprzestępcy dążą do zwabienia swoich ofiar i wyłudzenia od nich poufnych danych. Przykładowo, mogą fałszywie przekierowywać użytkowników na złośliwe witryny i prosić ich o podanie haseł oraz innych danych uwierzytelniających. Następnie pozyskane hasła mogą być wykorzystane przez hakerów do nieautoryzowanego logowania. Ten rodzaj ataku jest obecnie powszechnie stosowany, ponieważ jest stosunkowo łatwy do przeprowadzenia. Istnieje wiele różnych technik inżynierii społecznej, w tym phishing, vishing (phishing głosowy), a także bardziej zaawansowane manipulacje, które łączą różne techniki w celu osiągnięcia celu.

Ataki Brute Force to próby złamania hasła poprzez wypróbowanie wszystkich możliwych kombinacji znaków lub próby znalezienia aplikacji, która zaakceptuje skradzione hasło. W ramach tych ataków hakerzy wykorzystują tzw. ataki słownikowe, w których sprawdzają, czy któreś z popularnych i często używanych słów lub wyrażeń pasuje jako hasło. Aby znaleźć aplikację, która akceptuje skradzione hasło, hakerzy wykorzystują techniki takie jak "password spraying" lub "credential stuffing." W przypadku password spraying, atakujący używają krótkiej listy powszechnie używanych haseł, takich jak "12345678," próbując uzyskać dostęp do wielu różnych kont. Ich celem jest znalezienie dopasowania, które umożliwi im wejście na konto ofiary. Organizacje i dostawcy usług internetowych powinni wdrażać mechanizmy ochronne, które identyfikują i blokują podejrzane próby uwierzytelniania, aby zminimalizować ryzyko udanych ataków Brute Force.

Przechwytywanie danych wejściowych to technika wykorzystywana przez atakujących w celu uzyskania poufnych informacji, takich jak hasła, poprzez monitorowanie lub przechwytywanie procesu wprowadzania danych przez użytkowników. Atakujący mogą zainstalować keyloggery na komputerach ofiar. Keyloggery są programami lub urządzeniami, które rejestrują klawisze naciskane na klawiaturze. Dzięki temu atakujący uzyskują dostęp do wszystkich wprowadzanych przez użytkownika danych, w tym haseł. Atakujący mogą manipulować wyglądem interfejsu użytkownika, aby wydawało się, że wprowadzane dane trafiają do legalnej aplikacji lub systemu, podczas gdy tak naprawdę są przechwytywane przez złośliwe oprogramowanie. To zmyla ofiary i pozwala na zbieranie poufnych informacji.

Sniffing to technika przechwytywania danych, w której atakujący monitoruje ruch sieciowy w celu uzyskania poufnych informacji. Jest to działanie pasywne, co oznacza, że atakujący nie wprowadza aktywnie zmian w transmisji danych, ale jedynie podsłuchuje przesyłane informacje. Atakujący używa narzędzi, takich jak sniffer (program lub urządzenie do analizy ruchu sieciowego), aby przechwycić pakiety danych przesyłane w sieci. Przechwycone pakiety danych są analizowane w poszukiwaniu poufnych informacji, takich jak hasła, dane logowania, karty kredytowe, czy inne wrażliwe dane. Sniffer może składować pakiety, aby zrekonstruować komunikację, co pozwala na uzyskanie pełniejszego obrazu i dostęp do wrażliwych danych.

Ataki typu Man-in-the-Middle (MITM) są zaawansowanymi technikami, które pozwalają atakującemu na przejęcie i umieszczenie się w kanale komunikacyjnym między użytkownikami a aplikacjami lub usługami, z którymi się łączą. To oznacza, że haker znajduje się "w środku" komunikacji między dwiema stronami i może przechwytywać, modyfikować lub nawet fałszować przesyłane dane. Atakujący „umieszcza się” pomiędzy użytkownikiem a aplikacją lub serwerem, co pozwala mu na monitorowanie całej transmisji danych. Atakujący przechwytuje cały ruch sieciowy między użytkownikiem a aplikacją. To może obejmować przesyłane hasła, dane logowania, sesje, czy inne wrażliwe informacje. W zależności od celów ataku, atakujący może modyfikować dane przesyłane między dwiema stronami. Na przykład, może podmienić zawartość przesyłanej strony internetowej lub fałszować odpowiedzi serwera.

## Zabezpieczenia przed atakami

Atakujący nie jest w stanie podać się za kogoś innego, ponieważ te cechy biometryczne są unikalne dla każdej osoby. Jednak, istnieją wyzwania związane z zachowaniem prywatności i bezpieczeństwem danych biometrycznych, dlatego ważne jest, aby odpowiednio zabezpieczać i przechowywać te dane.

Aby chronić się przed przechwytywaniem danych wejściowych, ważne jest zastosowanie odpowiednich środków zabezpieczających, takich jak:

* Regularne skanowanie komputerów pod kątem keyloggerów i złośliwego oprogramowania.
* Używanie antywirusów i zapór ogniowych.
* Aktualizacja systemu operacyjnego i oprogramowania do najnowszych wersji.
* Wybieranie bezpiecznych i renomowanych źródeł oprogramowania.
* Uwrażliwienie na podejrzane sytuacje, takie jak zmiany w wyglądzie interfejsu użytkownika.

Aby zabezpieczyć się przed atakami sniffing, ważne jest stosowanie zabezpieczeń sieciowych, takich jak szyfrowanie danych (np. protokół HTTPS), monitorowanie i wykrywanie nieautoryzowanego dostępu do sieci oraz regularne aktualizacje systemów operacyjnych i oprogramowania w celu naprawienia znanych luk bezpieczeństwa. Warto również unikać korzystania z publicznych, niezabezpieczonych sieci Wi-Fi oraz stosować rozsądne praktyki, takie jak korzystanie z bezpiecznych haseł i unikanie przesyłania wrażliwych informacji w niezaszyfrowanej postaci.

Aby chronić się przed atakami typu MITM, ważne jest korzystanie z bezpiecznych protokołów komunikacyjnych, takich jak HTTPS, które zapewniają szyfrowanie danych. Ponadto, należy unikać korzystania z otwartych, niezabezpieczonych sieci Wi-Fi i stosować technologie zabezpieczające, takie jak wirtualne sieci prywatne (VPN). Dodatkowo, monitorowanie ruchu sieciowego w poszukiwaniu nieprawidłowości i podejrzanych zachowań może pomóc w wykryciu ataków MITM.

# Rozdział 5: Aplikacja do uwierzytelniania wieloskładnikowego

System uwierzytelniania wieloskładnikowego (MFA) stanowi kluczowy element w dzisiejszym środowisku cyfrowym, gdzie bezpieczeństwo danych i dostępu jest priorytetem. Przedstawiony system o nazwie **Be Safe Warrior** łączy różne metody uwierzytelniania, tworząc kompleksowe podejście do ochrony kont użytkowników. Niniejszy system został zaprojektowany w formie aplikacji webowej, umożliwiającej użytkownikom zarządzanie swoimi danymi uwierzytelniającymi w intuicyjny i efektywny sposób.

1. Rejestracja i Dodawanie Metod Uwierzytelniania:

Użytkownicy korzystają z aplikacji poprzez stronę www, gdzie mają możliwość utworzenia konta. Podczas tego procesu, zachęca się ich do dodawania różnych metod uwierzytelniania, takich jak hasła, klucze U2F, czy biometryka. To umożliwia zastosowanie wieloczynnikowego podejścia, co przekłada się na podniesienie poziomu bezpieczeństwa.

1. Sprawdzanie Siły Hasła:

Podczas tworzenia i aktualizowania haseł, system aktywnie ocenia ich siłę. Użytkownicy otrzymują natychmiastowe informacje dotyczące potencjalnych zagrożeń i zalecenia dotyczące wzmocnienia haseł, co zwiększa świadomość w zakresie bezpieczeństwa. Dodatkowo jest stworzona strona, na której można tworzyć hasła, a także badać ich siłę i różnorodnie modyfikować by stawały się silniejsze.

1. Edukacyjny Poradnik o Bezpieczeństwie:

Strona zawiera rozbudowany poradnik, który oferuje użytkownikom wskazówki dotyczące bezpiecznego korzystania z systemu i Internetu jako całości. Tematy obejmują ochronę hasła, identyfikację zagrożeń, aktualizacje oprogramowania, itp.

1. Integracja z Aplikacjami Zewnętrznymi:

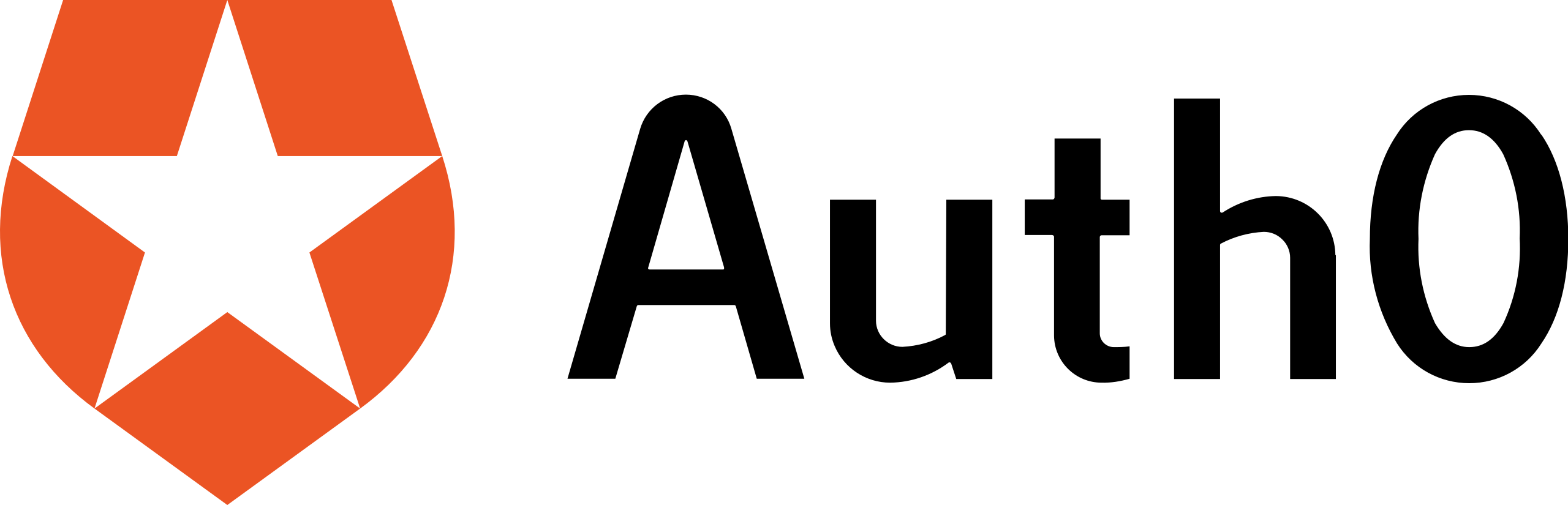
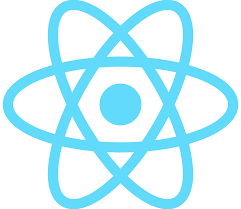
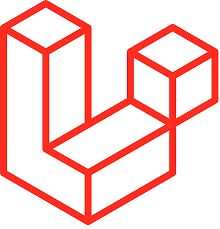
Aplikacja jest zoptymalizowana pod kątem integracji z innymi platformami i usługami, co umożliwia pełne wykorzystanie systemu MFA w różnych kontekstach.

1. Intuicyjny Interfejs Użytkownika:

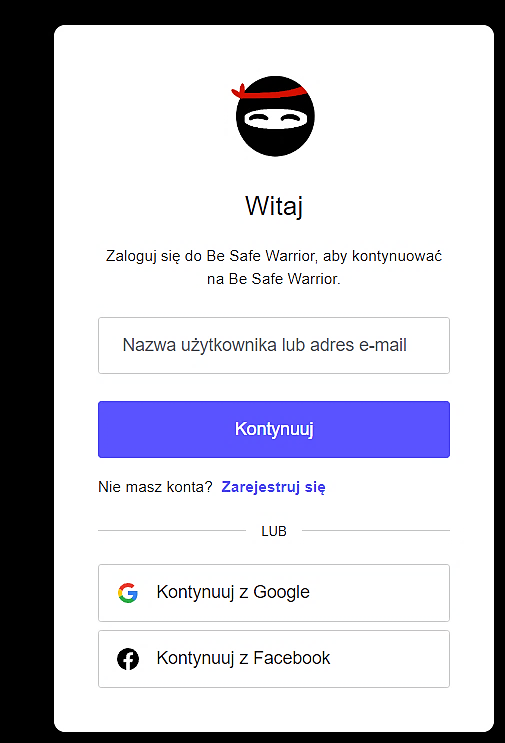
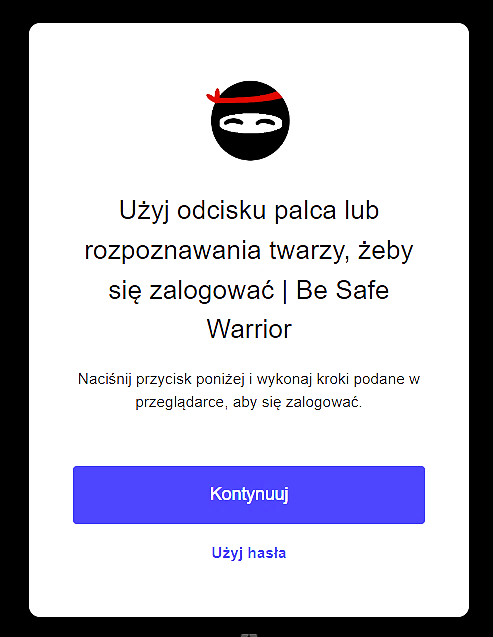
Aplikacja posiada prosty i intuicyjny wygląd, umożliwia łatwą nawigację i konfigurację konta. Jasne i zrozumiałe komunikaty dla użytkowników dotyczące procesu uwierzytelniania, ułatwiają zrozumienie całego procesu.

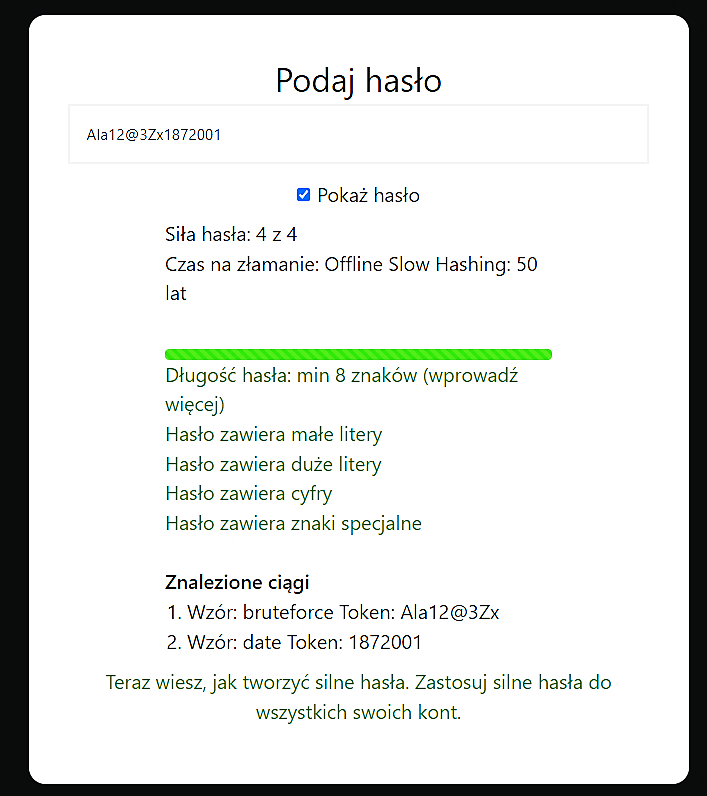
Aplikacja została przystosowana do wyświetlania na urządzeniach mobilnych, na których w większości są montowane czytniki linii papilarnych, więc można z nich korzystać w celu logowania się do swojego profilu.

Aplikacja została napisana z wykorzystaniem Laravel oraz React. Do strony napisanej w tych frameworkach zostały dołożony komponent znany jako Auth0, który umożliwia uwierzytelniać użytkownika i autoryzować my dostęp do zasobów strzeżonych na naszej stronie Be Safe Warrior.



Strona logowania:



Sprawdzanie siły hasła:

Sprawdzanie siły haseł odbywa się na dwa sposoby:

1. Sprawdzenie poszczególnych reguł:
   1. Długość hasła: min 8 znaków
   2. Hasło zawiera małe litery
   3. Hasło zawiera duże litery
   4. Hasło zawiera cyfry
   5. Hasło zawiera znaki specjalne

1.     const length = password.length;

2.     setdlugosc(length > 7 ? 'green' : 'red');

3.     const hasLowerCase = /[a-z]/.test(password);

4.     setmale\_litery(hasLowerCase ? 'green' : 'red');

5.     const hasUpperCase = /[A-Z]/.test(password);

6.     setduze\_litery(hasUpperCase ? 'green' : 'red');

7.     const hasNumber = /\d/.test(password);

8.     setcyfry(hasNumber ? 'green' : 'red');

9.     const hasSpecialChar = /[!@#$%^&\*(),.?":{}|<>]/.test(password);

10.     setspecjalne(hasSpecialChar ? 'green' : 'red');

11. if (length > 7 && male\_litery === 'green' && duze\_litery === 'green' && cyfry === 'green' && specjalne === 'green') {

12.       setkomunikat\_czas(<>Czas na złamanie: Offline Slow Hashing: {testResult.crackTimesDisplay.offlineSlowHashing1e4PerSecond}</>);

13.     }

1. Sprawdzenie siły poprzez zxcvbn

1. import { zxcvbn, zxcvbnOptions } from '@zxcvbn-ts/core'

2. import \* as zxcvbnCommonPackage from '@zxcvbn-ts/language-common'

3. import \* as zxcvbnPlPackage from '@zxcvbn-ts/language-pl'

4. const testResult = zxcvbn(password);

5. const inputType = showPassword ? 'text' : 'password';

6.

7. const handlePasswordChange = (event) => {

8. setPassword(event.target.value);

9. }

10. const handleCheckboxChange = () => {

11. setShowPassword(!showPassword);

12. };

13. const options = {

14. translations: zxcvbnPlPackage.translations,

15. graphs: zxcvbnCommonPackage.adjacencyGraphs,

16. dictionary: {

17. ...zxcvbnCommonPackage.dictionary,

18. ...zxcvbnPlPackage.dictionary,

19. },

20. }

21. zxcvbnOptions.setOptions(options)

22.

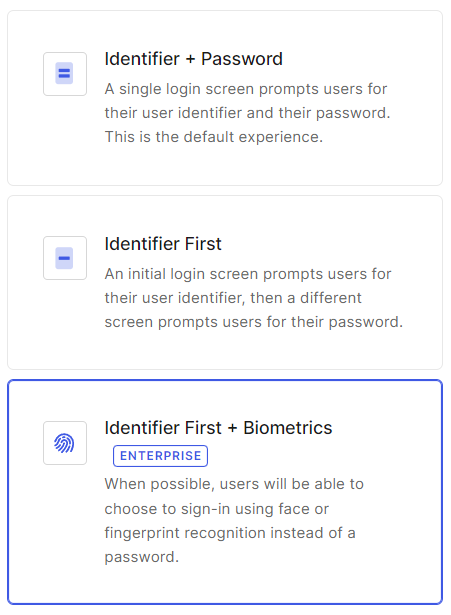
## Auth0

Auth0 to platforma za pomocą której można prowadzić procesy uwierzytelniania i autoryzacji. Udostępnia zestaw narzędzi, które umożliwiają programistom dodanie do swoich usług przepływów uwierzytelniania i autoryzacji do swoich aplikacji.

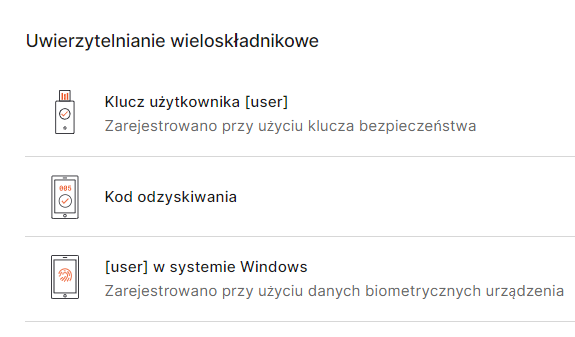
Usługa pozwala na dostęp do swojego profilu bez wykorzystania standardowego hasła. W zamian oferuje takie możliwości jak: uwierzytelnianie biometryczne (między innymi odcisk palca, skan twarzy), kody przekazywane przez SMS oraz na pocztę e-mail. Sprawia to, że uwierzytelnianie przebiega w bezpieczniejszy sposób, ponieważ rezygnuje się ze standardowego hasła, które można wykraść w różnoraki sposób. Eliminuje to potrzebę zapamiętywania wszystkich haseł i zarządzania nimi, dzięki czemu zmniejszamy ryzyko naruszenia bezpieczeństwa haseł.

Wykorzystując Auth0 można logować się na stronie za pomocą innych kont utworzonych w różnych serwisach takich jak: Facebook, Google. Te dwie zostały dołączone do aplikacji, a możliwych innych sposób jest znacznie więcej, bo jest to aż 70 różnych opcji logowania społecznościowego.

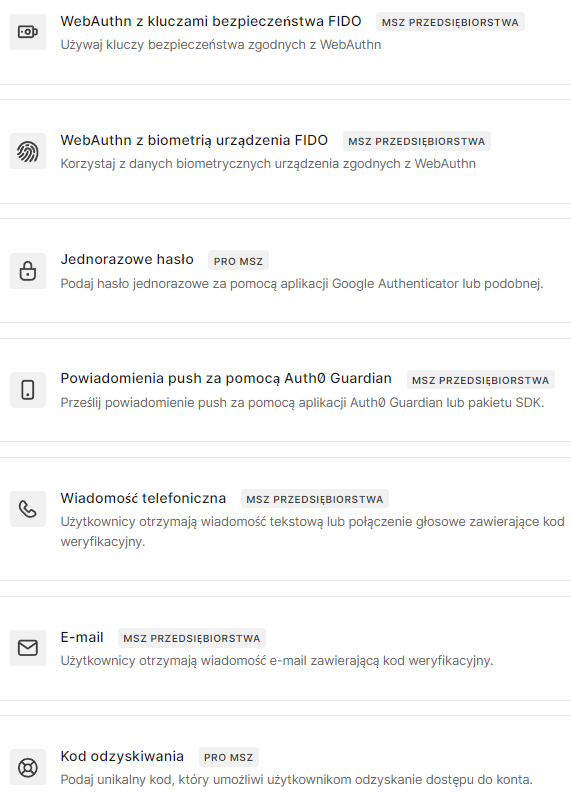
Auth0 można zintegrować z dowolną aplikacją lub witryną internetową, niezależnie od stosu technologii, języka programowania i struktury. Auth0 zapewnia proste rozwiązania integracyjne, które wymagają od programistów minimalnego czasu i wysiłku. Programiści mogą bezpiecznie łączyć Auth0 z istniejącymi interfejsami API za pośrednictwem panelu administracyjnego. Platforma ułatwia programistom definiowanie istniejącego API, konfigurowanie reguł autoryzacji i dodawanie tokenu dostępu do kodu istniejącej aplikacji.



W panelu administratora można modyfikować sposoby, w jakie strona ma uwierzytelniać użytkownika. Może to być tylko login i hasło na jednej stronie. Drugą opcją jest podanie samego loginu, a jeżeli znajduje się w bazie danych, to dalej może kontynuować bez wykorzystania hasła. Trzecią opcją jest podanie identyfikatora, a następnie biometrii, klucza U2F lub innych czynników.



Aplikacja pozwala na zarządzanie użytkownikami, modyfikowaniem ich danych, a także dokładaniu metadanych, czy określeniu ról jakie dany użytkownik ma spełniać. Pokazują się tu także informacje o tym, jakie sposoby są wykorzystywane w uwierzytelnianiu wieloskładnikowym.

Uwierzytelnianie wieloskładnikowe wymaga dodatkowych czynników podczas procesu logowania, aby zapobiec nieautoryzowanemu dostępowi. Dostępne czynniki:

# Rozdział 6: Podsumowanie i Wnioski

W miarę, jak technologia staje się coraz bardziej połączona z naszą codziennością, zwiększanie bezpieczeństwa i uwierzytelniania stają się kluczową kwestią. Systemu uwierzytelniania odgrywają istotną rolę, ponieważ zabezpieczają nasze dane, nasze pliki, a także konta na różnych serwisach internetowych, ale także konta w systemach operacyjnych.

Należy przyjrzeć się obecnemu poziomowi zabezpieczeń naszych kont i danych, by mieć pewność, że są chronione w wystarczający sposób. Powinno się dokonać analizy haseł i loginów do wszystkich kont z których korzystamy, a następnie zwiększyć ich bezpieczeństwo poprzez zastosowanie silnego hasła, różnych haseł do różnych stron, wdrożenia uwierzytelniania wieloetapowego z wykorzystaniem na przykład biometrii. Im więcej składników uwierzytelniania wdrożymy, tym mocniej będziemy chronieni.

Jednakże należy zachować równowagę pomiędzy bezpieczeństwem a wygodą. Chcąc logować się to serwisu społecznościowego, nie musimy używać do obecnego loginu i hasła zbyt wielu czynników. Gdyż znacząco utrudnimy sobie życie. Czy posiadanie loginu i hasła, następnie tokenu sprzętowego na dodatkowym urządzeniu, a finalnie jeszcze odcisku palca w aplikacji mobilnej na naszym smartfonie to nie jest zbytnie przesadzenie w jedną stronę? Czy nie lepiej tam, gdzie jest to konieczne wdrażać więcej zasad bezpieczeństwa, a tam gdzie nie jest to konieczne zwyczajne, proste, ale wystarczająco silne zabezpieczenia?

Wśród społeczeństwa należy przeprowadzać szkolenia i edukować ludzi, by potrafili zachować bezpieczeństwo w sieci, ale także umiejętnie chronili swoje dane. Wiele osób posiada krótkie i nieskomplikowane hasła, które początkujący haker może zdobyć w ciągu kilku godzin. Zwłaszcza starsze społeczeństwo, dla których technologia jest czymś nowym, powinny zostać uświadomieni z zagrożeniami jakie na nich czekają.

Zagrożeń w dzisiejszym wirtualnym świecie jest bardzo dużo i na każdym kroku człowiek jest narażony na ataki, zwłaszcza na phishing, a stron podszywających się pod oryginalne instytucje jest cała masa. Podamy nasze dane logowania na stronie, która podszywa się pod nasz bank, jest niemalże równoznaczne z tym, że utracimy wszystkie środki na nim zgromadzone. A odróżnienie strony oryginalnej to kopii nie jest proste dla osób, które nie wiedzą, że coś takiego może istnieć. Dlatego należy wystrzegać się wszystkich sms, połączeń i e-maili, które wyglądają na podejrzane i pod żadnym pozorem nie podawać swoich danych. W takich sytuacjach należy skontaktować się z oryginałem strony i zgłoszenie próby wyłudzenia danych.

# Bibliografia

<https://cybersecurity.asee.co/blog/history-of-authentication/>

<https://iist.uwb.edu.pl/~m.rybnik/wp-content/uploads/BDiSI-W3.pdf>

<https://forumcallcenter.pl/wp-content/uploads/2017/11/ICT-Biometria-Whitepaper-PL.pdf>

<https://www.simplilearn.com/modern-authentication-vs-basic-authentication-article>

<https://www.citrix.com/solutions/secure-access/what-is-adaptive-authentication.html>

<https://www.intechopen.com/journals/1/articles/100>

<https://www.mdpi.com/2075-4418/13/3/439>

adresy grafik:

<https://media.licdn.com/dms/image/C4D12AQGIT26AaErPAw/article-inline_image-shrink_1500_2232/0/1637760690696?e=1703721600&v=beta&t=Q4DooYEbBxYTYNDe8WlP-1Y5OrbrGuUt3Osef4nRp8M>

<https://www.researchgate.net/publication/333577951/figure/fig1/AS:866473572581376@1583594806690/Multi-Factor-Authentication-Source-Adapted-from-Lambauer-2016.ppm>

<https://static.credit-agricole.pl/asset/t/o/k/token-sprzetowy-zatwierdzanie-1_25608.webp>

<https://edu.pjwstk.edu.pl/wyklady/tbo/scb/lecture-12/images/image-12-01.gif>

<https://edu.pjwstk.edu.pl/wyklady/tbo/scb/lecture-12/images/image-12-02.gif>

<https://edu.pjwstk.edu.pl/wyklady/tbo/scb/lecture-12/images/image-12-03.gif>

kod brute force: https://www.w3resource.com/python-exercises/cybersecurity/python-cybersecurity-exercise-10.php