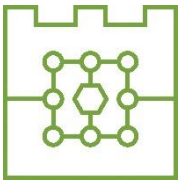
Politechnika Krakowska

im. Tadeusza Kościuszki

Wydział Informatyki i Telekomunikacji



Jan Chmielewski

Numer albumu: 133496

Analiza różnych metod autoryzacji w aplikacjach mobilnych na system Android

Analysis of various authorization methods in mobile applications on the Android system

Praca magisterska

na kierunku INFORMATYKA

specjalność CYBERBEZPIECZEŃSTWO

Praca wykonana pod kierunkiem:

dr Radosława Kyci

oraz pod opieką:

mgr inż. Łukasza Gaży

Kraków, 2024

Spis treści

Wykaz ważniejszych oznaczeń i skrótów

SWOT – technika analizy, której elementami składowymi są silne strony (*strenghts*), słabe strony (*weaknesses*), szanse (*opportunities*) oraz zagrożenia (*threats*) [1]

TOWS – technika analizy oparta na SWOT, ale mająca podejście „z zewnątrz do wewnątrz" gdzie w pierwszej kolejności zwracana jest uwaga na czynniki zewnętrzne [2]

MFA – Multi Factor Authentication

PIN – Personal Identification Number

ISO – International Organization for Standarization

NFC – Near Field Communication – standard komunikacji bezprzewodowej oparty na technologii zbliżeniowej

Autoryzacja – inaczej upoważnienie, przyznanie dostępu do konkretnego zasobu, do którego użytkownik jest uprawniony [3]

Autentykacja – inaczej uwierzytelnienie, proces weryfikacji tożsamości lub innych atrybutów zgłaszanych przez użytkownika [4]

Rola autoryzacji we współczesnym świecie

Niezaprzeczalnym faktem w dzisiejszym świecie jest to, że smartfony i inne urządzenia określane jako inteligentne (z ang. *smart*) są narzędziami codziennego użytku, z których korzysta zdecydowana większość społeczeństwa. Urządzenia te od dawna przestały pełnić funkcję wyłącznie narzędzi służących do komunikacji na odległość, a stały się również kartami płatniczymi czy pilotami do bram, nie wspominając już o wiadomościach tekstowych i poczcie mailowej, które zawierają ogromną ilość wrażliwych informacji. W ciągu całego dnia z pewnością każdemu zdarzy się zostawić swój telefon bez nadzoru, czy to na stole podczas parzenia kawy w kuchni pracowniczej, czy też w parku na ławce szukając czegoś w plecaku. Urządzenia można też najzwyczajniej w świecie zgubić, a biorąc pod uwagę ich zawartość należy zastanowić się nad tym czy są one dostatecznie zabezpieczone przed dostępem osób niepowołanych? Gdyby każdemu użytkownikowi przedstawić jakie dane znajdują się w jego smartfonie i jakie skutki mogłaby przynieść ich utrata, zdecydowanie znalazłaby się część osób która zastanowiłaby się dwa razy przed ustawieniem kolejny raz w nowym telefonie słabego kodu PIN. Według danych zebranych z wycieków kodów PIN z różnych baz danych, w pierwszej trójce najpopularniejszych kodów znajdują się wręcz trywialne kombinacje, są to kolejno „1234”, „1111” oraz „0000” [5]. Stanowiły one razem prawie 19% wszystkich zgromadzonych kodów, co obrazuje skalę problemu wybierania prostych haseł przez użytkowników kierujących się bardziej wygodą niż bezpieczeństwem.

Producenci systemów mobilnych stworzyli wiele sposobów autoryzacji, tak aby użytkownicy mogli wybrać ten który będzie dla nich najbardziej wygodny, zapewniając przy tym odpowiedni poziom zabezpieczeń, gwarantowany przez mechanizmy odpowiedzialne za ich działanie. Metody te ewoluowały na przestrzeni lat, również z powodu luk w zabezpieczeniach, nierzadko odkrywanych dopiero po ich wykorzystaniu przez osoby o nieczystych intencjach. Również obecne sposoby autoryzacji są narażone na naruszenia bezpieczeństwa i dlatego tak ważne jest poddawanie ich ciągłej analizie mającej na celu ponowne badanie ich możliwości i ograniczeń oraz ewentualną aktualizację pod kątem znalezionych słabych stron.

Cel pracy

Niniejsza praca ma na celu zbadanie metod autoryzacji dostępnych w systemie operacyjnym na urządzenia mobilne o nazwie Android [6] pod kątem bezpieczeństwa, a w szczególności możliwości wykorzystania ich słabych stron w celu uzyskania dostępu do zabezpieczonego urządzenia, oraz jak może ona uchronić użytkownika korzystając ze swoich zalet. Analiza ta być może umożliwi wyłonienie spośród nich metod skrajnie niebezpiecznych jak również metod o wybitnie wysokim poziomie bezpieczeństwa

Zakres pracy

W pracy przytoczona zostanie niezbędna wiedza teoretyczna dotycząca poszczególnych metod autoryzacji i ich działania. Następnie metody te poddane zostaną analizie, podczas której wykorzystane zostaną odpowiednie metody badawcze . Na końcu wyniki analizy zostaną podsumowane i wyciągnięte zostaną wnioski.

Metodyka

Podczas analizy wykorzystana zostanie technika SWOT/TOWS w celu uporządkowania i teoretycznego zbadania metod autoryzacji. Będzie ona miała na celu przedstawienie charakterystyk wszystkich metod, ze zwróceniem uwagi na ich silne strony oraz słabe punkty, wpływające bezpośrednio na ich poziom bezpieczeństwa.

I. Część teoretyczna

Poniższa część pracy skupiać się będzie na przedstawieniu poszczególnych metod autoryzacji zaimplementowanych w systemie Android. Omówione zostaną mechanizmy działania każdej z metod, z przytoczeniem odpowiedniej wiedzy teoretycznej niezbędnej do ich zrozumienia, a także statystyk ich popularności wśród użytkowników.

1. Wprowadzenie

Przed przystąpieniem do przeglądu metod autoryzacji konieczne jest zdefiniowanie podstawowych terminów użytych w niniejszej pracy. Wcześniejsze ich przedstawienie ma na celu ułatwić czytelnikowi zrozumienie omawianych w pracy zagadnień związanych z bezpieczeństwem użytkownika w systemie Android.

1.1. Autoryzacja a autentykacja

Autoryzacja i autentykacja to dwa kluczowe pojęcia pojawiające się w niniejszej pracy. Istotne jest zrozumienie różnic występujących między nimi.

Autoryzacja jest to proces przyznawania użytkownikowi uprawnień do wykorzystania określonych zasobów czy funkcji systemu. W kontekście systemu Android może to dotyczyć dostępu do danych, aplikacji lub funkcji urządzenia jak np. wrażliwe ustawienia systemowe. Autoryzacja następuje po prawidłowym przejściu procesu autentykacji, który potwierdza tożsamość użytkownika [3].

Autentykacja to weryfikacja tożsamości użytkownika, polegający na sprawdzeniu, czy osoba próbująca uzyskać dostęp do zasobów faktycznie jest tym, za kogo się podaje [4].

1.2. Metoda odblokowania

W kontekście urządzeń mobilnych, *metoda odblokowania* odnosi się do technik wykorzystywanych w celu uzyskania dostępu do urządzenia chronionego przed dostępem osób trzecich. Jest to dokładniej mówiąc pewna metoda autoryzacji, o określonym zasobie do jakiego uzyskiwany jest dostęp, który stanowi np. smartfon, tablet czy laptop. Dopiero po uzyskaniu do nich dostępu możliwe jest wykonywanie jakichkolwiek operacji na tych urządzeniach.

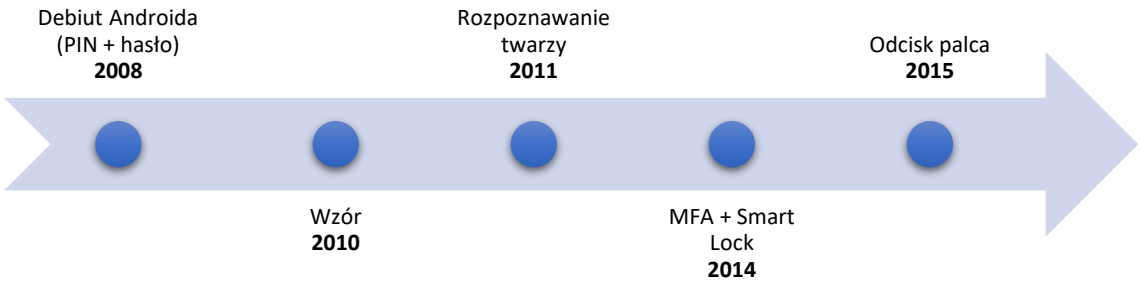
1.3. Metody ataków

Dostępne w systemie Android metody autoryzacji narażone są na kompromitację w wyniku różnego rodzaju ataków. Wśród nich najpopularniejszymi są:

- *Brute force* – jest to systematyczna próba złamania danego zabezpieczenia przez sprawdzanie wszystkich możliwych kombinacji hasła czy kodu PIN, aż do znalezienia tej poprawnej. Atakowi takiemu przeciwdziałać można przez limitowanie prób do pewnej ilości i wymuszanie przerw czasowych lub całkowitą blokadę urządzenia. Atak ten potrafi być bardzo czasochłonny, dlatego im większa jest maksymalna złożoność danej metody autoryzacji, tym bardziej może to zniechęcić potencjalnych atakujących.
- *Shoulder surfing* – technika, która polega na obserwowaniu użytkownika w celu podglądnięcia wpisywanego hasła, wzoru czy kodu PIN. Może być realizowana przez obserwację bezpośrednią np. stojąc za nim, lub pośrednią z wykorzystaniem kamer zainstalowanych w pobliżu.
- *Phishing* – polega na wyłudzeniu poufnych informacji jak hasła czy kody uwierzytelniające, poprzez podszywanie się pod zaufane osoby, firmy, instytucje. W systemie Android możliwe jest również wykorzystanie fałszywych aplikacji lub wiadomości tekstowych które zachęcają do przekazania swoich danych. Istotne jest aby weryfikować nadawców wiadomości, oraz instalować aplikacje wyłącznie z zaufanych źródeł.
- *Deep fake* – agresywny rozwój w sektorze sztucznej inteligencji wpłynął na udoskonalenie generowania realistycznych obrazów lub filmów, które mogą posłużyć przestępcom do złamania zabezpieczeń biometrycznych lub w celu wyłudzenia danych poprzez phishing.

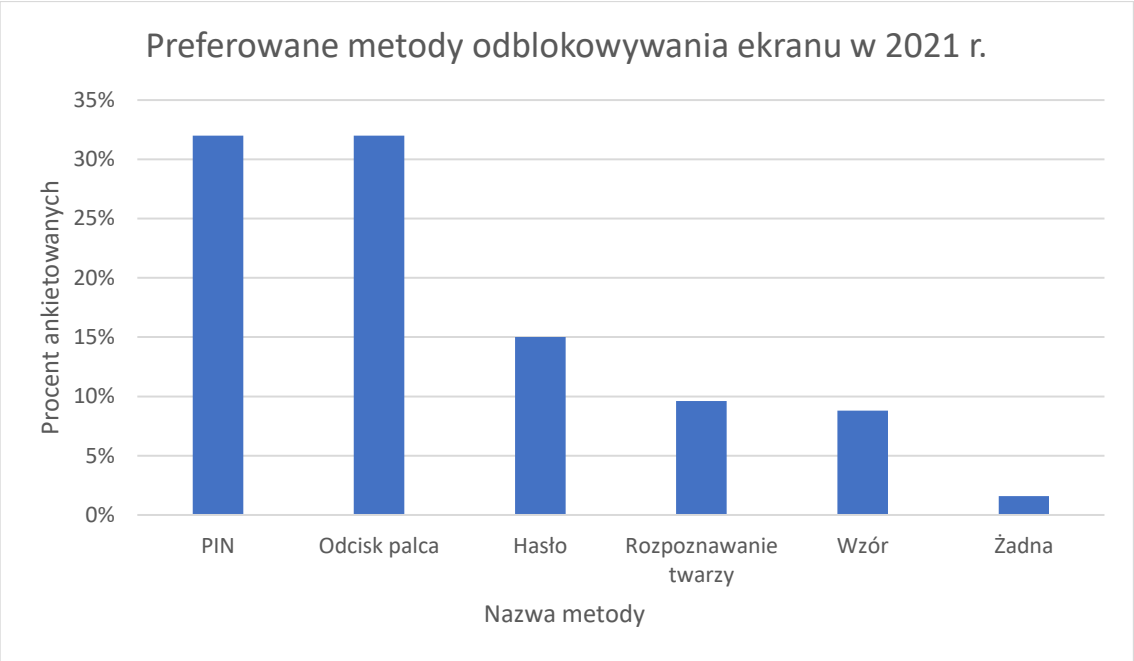
2. Przegląd metod autoryzacji w systemie Android

W niniejszym rozdziale przedstawione zostaną istniejące metody autoryzacji i autentykacji dostępne na platformie Android. Dostęp do poszczególnych metod oraz ich implementacje mogą się różnić w zależności od producenta urządzenia oraz rynku na jakim jest ono oferowane. Na przestrzeni lat pojawiały się coraz to nowsze sposoby zabezpieczeń aplikacji, a te już istniejące ewoluowały zmieniając się w mniejszym lub większym stopniu. Poniższa oś czasu na Rysunku 1.1 przedstawia lata w których omawiane metody debiutowały na platformie od Google:



Rysunek 2.1 Przedstawienie metod autoryzacji na osi czasu, źródło: opracowanie własne

Wykres na Rysunku 1.2 prezentuje natomiast statystyki dotyczące preferowanego sposobu odblokowania urządzenia wśród osób dorosłych na świecie w 2021 roku.



Rysunek 2.2 Wykres preferowanych metod odblokowywania ekranu w 2021 r., źródło: https://www.statista.com/statistics/1305993/screen-lock-methods-global-users/ , dostęp 09.09.2024

2.1. Odblokowywanie kodem PIN

Personal Identification Number znany powszechnie jako PIN, jest jedną z najpopularniejszych na świecie metod zabezpieczania dostępu, nie tylko do urządzeń elektronicznych – na podobnych numerycznych hasłach opierają się kody do drzwi, kłódek czy sejfów. Ten krótki, najczęściej 4 znakowy kod, składa się wyłącznie z cyfr co powoduje, że jest dość prosty w zapamiętaniu, a zakładając że jest znany jedynie osobie która go wymyśliła, jest jednym ze sposobów na potwierdzenie jej tożsamości. Niestety, ta sama osoba jest również słabym punktem tego mechanizmu – poziom bezpieczeństwa kodu PIN rośnie wraz z jego długością, a użytkownicy najczęściej pozostają przy minimalnej długości czterech cyfr określonej w standardzie ISO 9564-1 [7]. Drugim istotnym aspektem poddającym bezpieczeństwo tej metody w wątpliwość jest fakt, iż kody wymyślane przez ludzi często są proste w odgadnięciu bo np. są związane z ich datą urodzenia, lub wręcz trywialne jak „1111” – mając dostęp do danych o najczęściej używanych przez użytkowników kodach PIN, można znacząco skrócić czas potrzebny na jego złamanie poprzez optymalizację sprawdzanych sekwencji zamiast losowych prób odgadnięcia hasła. Ostatnim elementem wpływającym na poziom ochrony tej metody autentykacji, a o którym wielu użytkowników nawet nigdy nie słyszało jest regularna

zmiana kodu. Może to zapobiec uzyskaniu dostępu do urządzenia osobie, która w jakiś sposób pozyskała kod PIN używany przez ofiarę w sprzęcie sprzed kilku lat, lub zwyczajnie używany na innym urządzeniu tej samej osoby. Niestety taka sytuacja jest bardzo powszechna wśród użytkowników, którzy dla oszczędzenia sobie zapamiętywania wielu różnych kodów PIN używają tego samego zarówno do telefonu, karty płatniczej oraz systemu alarmowego w domu. Skutki wycieku tego jednego kodu mogą być w takim przypadku katastrofalne.

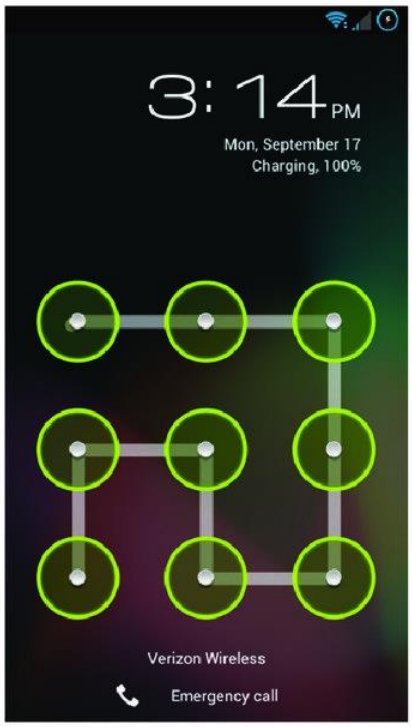
2.2. Zabezpieczenie hasłem

Hasło było drugą po kodzie PIN metodą z jaką debiutował system Android. W przeciwieństwie do niego może się ono jednak składać z cyfr oraz liter i znaków specjalnych co w znaczący sposób zwiększa jego potencjał bezpieczeństwa. Obecnie wymagana długość hasła dla systemu Android wynosi co najmniej 4 lub 6 znaków, zależnie od ustawień polityki bezpieczeństwa w danym urządzeniu [8]. Jednakże pomimo innej zasady tworzenia hasła niż w przypadku kodu PIN, jest ono narażone na identyczne zagrożenia. Użytkownicy wciąż mogą stworzyć hasło zbyt krótkie, za łatwe lub, co jest niestety bardzo powszechne, stosować jedno hasło do wszystkich swoich urządzeń i kont. Metoda ta z powodu swojej większej złożoności powodowanej większym zakresem możliwych znaków do wpisania, jest też bardziej uciążliwa w codziennym użytkowaniu przez co wiele osób decyduje się wybrać inne, szybsze metody odblokowywania telefonu. Wpisanie długiego hasła podczas logowania na stronie internetowej nie jest problematyczne, natomiast biorąc pod uwagę, że przeciętny użytkownik smartfonu odblokowuje go średnio 79 razy dziennie [9], niska popularność tej metody autentykacji jest całkowicie zrozumiała.

2.3. Wzór jako blokada ekranu

Odblokowanie wzorem to opatentowana przez firmę Google metoda zabezpieczenia dostępu do urządzenia, wprowadzona w 2009 roku do systemu Android w aktualizacji 2.0 „*Eclair*”. Polega ona na wykorzystaniu matrycy pól o rozmiarze 3x3 oraz kombinacji składających się z połączeń tych pól o długości nie mniejszej niż 4 i nie większej niż 9

[10]. Rozmiar siatki nie jest możliwy do modyfikacji, jest to wykonalne jedynie w zmodyfikowanych wersjach systemu, które użytkownicy mogą samodzielnie wgrać na swoje urządzenia, jednakże nie jest to zadanie z którym poradziliby sobie przeciętni użytkownicy nieposiadający odpowiedniej wiedzy technicznej. Pierwotny wygląd ekranu z blokadą opartą na wykorzystaniu wzoru przedstawia poniższy Rysunek 1.3.



Rysunek 2.3 Ekran blokady systemu Android z pierwszą wersją blokady wzorem, źródło: https://www.researchgate.net/figure/The-default-Android-grid-lock-showing-a-lock-pattern-for-a-33-grid_fig3_311163812 , dostęp 09.09.2024

Metoda ta zyskała na popularności wśród użytkowników dzięki wygodzie jaką oferowała – narysowanie gestem wzoru składającego się nawet z 6 elementów może być szybsze niż wpisanie czteroznakowego kodu PIN, zapewniając przy tym łatwość użycia oraz zadowalający poziom bezpieczeństwa. Oczywiście poziom zabezpieczeń wzrasta wraz z długością wzoru. Dodatkowe konfiguracje pozwalające np. na ukrycie wprowadzanego wzoru mogą jeszcze bardziej zabezpieczyć poufność wzoru użytkownika, czyniąc go trudniejszym do odczytania przez niepożądanych obserwatorów. Zdefiniowany przez użytkownika wzór nie powinien być również zbyt prosty, co diametralnie zwiększa szanse na jego odgadnięcie.

Do momentu wprowadzenia odblokowania poprzez odcisk palca, metoda odblokowania wzorem była najchętniej stosowaną przez użytkowników.

2.4. Czytniki linii papilarnych

Odblokowanie przy pomocy odcisku palca to aktualnie na równi z kodem PIN najbardziej popularna metoda odblokowywania urządzenia. Zaprezentowana została w 2015 roku wraz z wydaniem Androida 6.0 „*Marshmallow”* i jest wciąż rozwijana. Zauważyć można z pewnością znaczący wzrost prędkości oraz precyzji odczytywania linii papilarnych przez czytniki, czy możliwość zapisania w urządzeniu wielu odcisków palców. W obecnych czasach czytnik ten jest standardowym wyposażeniem każdego urządzenia osobistego. Na przestrzeni lat zmieniał on swoją formę i miejsce – pojawiały się czytniki wbudowane w przycisk włączania/wyłączania, umiejscowione na tylnej klapce telefonu, czy tak jak w najnowszych iteracjach schowane pod ekranem głównym – ale zasada działania pozostała niezmiennie ta sama. Czytnik po uprzednim skonfigurowaniu przy każdorazowym odblokowaniu skanuje linie papilarne i decyduje o autoryzacji operacji. Metoda ta zapewnia wysoki poziom bezpieczeństwa, ponieważ odcisk palca jest unikalną cechą biometryczną, trudną do zreprodukowania. W tym przypadku bezpieczeństwo nie zostało uzyskane kosztem wygody, ponieważ jest ona również na wysokim poziomie, a różnorakie umiejscowienie czytników w urządzeniach oferowanych przez producentów pozwala na dobranie odpowiedniego do własnych upodobań. Na wygodę wpływa również możliwość wykorzystania czytnika linii papilarnych jako bezpośredniego wyzwalacza włączenia ekranu, co eliminuje wcześniejszy krok naciśnięcia przycisku, w ten sposób optymalizując proces, który jak wspomniano we wcześniejszym rozdziale, jest powtarzany codziennie prawie 80 razy.

2.5. Rozpoznawanie twarzy użytkownika

Funkcja rozpoznawania twarzy została wprowadzona do systemu Android wraz z aktualizacją do wersji 4.0 „*Ice Cream Sandwich”.* Metoda ta polega na odblokowaniu urządzenia poprzez skierowanie na swoją twarz obiektywu przedniego aparatu. Ta technologia, będąca formą biometrycznego uwierzytelniania, miała zapewnić szybki i

wygodny dostęp do urządzenia bez konieczności wpisywania kodów PIN czy haseł. Jednakże pierwsze wersje tej metody były narażone na pewne luki bezpieczeństwa. Początkowe iteracje oprogramowania można było łatwo oszukać przy pomocy zwykłego zdjęcia lub nagrania wideo właściciela urządzenia. Przez to właśnie była uważana za mniej bezpieczną w porównaniu do innych form autoryzacji, pomimo swojej pozornej wygody. Pozornej, ponieważ nierzadko na odblokowanie urządzenia trzeba było poczekać co najmniej kilka sekund zanim aparat wychwycił twarz użytkownika, zwłaszcza przy niekorzystnych warunkach oświetleniowych. Kilka sekund trzymania urządzenia przed twarzą może wydawać się niewielkim problemem, ale w obecnych czasach i przy innych metodach których czas odblokowania zamyka się w niecałej sekundzie, jest to czas statystycznie o kilkaset procent większy. Aby zwiększyć poziom bezpieczeństwa tej metody Google udoskonaliło algorytm o funkcję, która wymagała od użytkownika mrugnięcia oczyma – był to tak zwany *liveness check*. Poprawka ta jednak nie zniwelowała wszystkich zagrożeń bezpieczeństwa a także nie wpłynęła na zwiększenie jej popularności wśród użytkowników. Z tego też względu aktywny rozwój tej metody autentykacji został zaniechany i skierowany na inne, również opierające się na biometrii, w szczególności czytniki linii papilarnych. W systemie Android pojawiały się jeszcze próby reaktywacji odblokowywania twarzą w nieco zmodyfikowanych odsłonach – Samsung wprowadził skaner tęczówki oka [11], Huawei trójwymiarowe skanowanie twarzy [12], a Google eksperymentowało z kamerami na podczerwień, projektorami i radarami [13], jednakże żadne z tych podejść nie odniosło znaczącego sukcesu na rynku i wkrótce później niektóre zniknęły z asortymentu producentów.

2.6. Smart Lock – inteligentne sposoby odblokowywania urządzenia

Smart Lock to kolejne ze strony firmy Google podejście do kompromisu pomiędzy wygodą użytkownika a względnie wysokim poziomem bezpieczeństwa. Funkcjonalność wprowadzona w 2014 roku wraz z aktualizacją systemową 5.0 *„Lolipop”* pozwala na automatyczne odblokowanie urządzenia w określonych sytuacjach. Pierwszą z nich jest sytuacja, kiedy do urządzenia użytkownika jest podłączone poprzez Bluetooth inne, określone wcześniej, zaufane urządzenie jak np. system głośnomówiący samochodu. Ułatwia to zdecydowanie szybkie skorzystanie z urządzenia podczas jazdy, co mniej

rozprasza kierującego pojazdem. Opcja ta może też mieć jednak negatywne skutki w sytuacji gdy nasze zaufane urządzenie znajduje się w pobliżu, ale niedostatecznie kontrolujemy kto może mieć dostęp do naszego telefonu co może ułatwić osobom niepożądanym bezproblemowy wgląd w jego zawartość. Kolejną dopuszczaną przez Smart Lock sytuacją jest ta, gdy urządzenie znajduje się w znanej lokalizacji zdefiniowanej przez użytkownika, np. pod adresem domowym. System wykorzystując sygnał GPS oraz Wi-Fi określa czy jest w bezpiecznej lokalizacji a następnie odblokowuje urządzenie, aż do momentu opuszczenia tej strefy. Tutaj również bezpieczeństwo tej metody zależy w głównej mierze od właściciela urządzenia. To on określa jakie miejsca telefon ma uznawać za zaufane i o ile dom jest przestrzenią względnie bezpieczną to już ustawienie miejsca pracy wyłącznie dla własnej wygody jest decyzją niekoniecznie rozsądną, jeżeli w pobliżu znajduje się wielu współpracowników i nie tylko. Ostatnią obsługiwaną sytuacją jest wykrycie kontaktu z ciałem. Polega ona na tym, że kiedy po odblokowaniu urządzenia będzie ono pozostawało w ruchu, np. w ręce czy kieszeni właściciela, to przy kolejnym włączeniu ekranu smartfon będzie automatycznie odblokowany. Ekran zablokuje się dopiero w momencie odłożenia urządzenia lub po 4 godzinach ciągłego odblokowania. W opinii autora niniejszej pracy jest to najbardziej wątpliwa metoda spośród zapewnianych przez Smart Lock, ponieważ nie jest ona w stanie rozpoznać czy urządzenie przebywa aktualnie w rękach właściciela, czy może ktoś inny przejął je bezpośrednio od niego, zachowując przy tym odblokowany ekran. Również producent tego rozwiązania ostrzega przed taką sytuacją w momencie włączania tej opcji. W przeciwieństwie do dwóch pozostałych metod które bazują na sprawdzaniu adresów MAC urządzeń lub koordynatów GPS, ludzie nie posiadają czytelnych dla sprzętów elektronicznych numerów po których mogłyby one weryfikować ich uprawnienia. Tak więc Smart Lock to metoda w pierwszej kolejności stawiająca wygodę użytkownika, a dopiero później bezpieczeństwo jego danych, które w znaczącym stopniu zależy od tego w jaki sposób on ją skonfiguruje.

2.7. Dodatkowe czynniki autentykacji

Autentykacja wieloskładnikowa to zaawansowany mechanizm bezpieczeństwa stosowany nie tylko w systemie Android. Jest to silna warstwa ochrony, która wymaga od użytkownika dostarczenia więcej niż jednego rodzaju dowodu tożsamości w celu

autoryzacji żądanej operacji. Należy zaznaczyć, że MFA w systemie Android najczęściej nie jest wykorzystywane jako metoda odblokowywania urządzenia, lecz jako autoryzacja w aplikacjach wymagających wysokiego poziomu bezpieczeństwa, który ta metoda zapewnia jak np. aplikacje bankowe, komunikatory. W systemie firmy Google rozwiązanie to zadebiutowało w wersji 5.0 *„Lolipop”*. Na metody mogące być wykorzystanymi jako czynniki MFA w różnej kombinacji składają się między innymi hasło, kod PIN, odcisk palca, kody jednorazowe czy fizyczne klucze sprzętowe. Dokładniej omówione zostaną dwie ostatnie z wymienionych metod z uwagi na to, że pozostałym zostały poświęcone osobne rozdziały w niniejszej pracy, oraz że zarówno kody jednorazowe jak i klucze sprzętowe zazwyczaj nie są wykorzystywane jako osobne, samowystarczalne metody autoryzacji.

Kody jednorazowe przesyłane za pomocą wiadomości SMS czy e-mail, są powszechnie spotykane podczas logowania do różnych kont internetowych. Są chyba jednym z popularniejszych czynników autoryzacji o niskim poziomie zaawansowania z perspektywy użytkownika końcowego. Polegają jedynie na przepisaniu kodu znajdującego się w wiadomości do wyznaczonego pola w aplikacji. Ich zaletą jest to, że dostęp do skrzynki odbiorczej oraz wiadomości tekstowych mamy praktycznie w każdym momencie, co nie jest tak oczywiste w przypadku kluczy sprzętowych stanowiących fizyczne urządzenie, zazwyczaj przypominające pendrive z uwagi na obecne złącze USB. Urządzenie takie zezwala na autoryzację danej akcji dopiero w momencie podłączenia lub zbliżenia do urządzenia jeżeli obsługuje komunikację po NFC. W ten sposób, nawet jeżeli niepożądana osoba uzyska pierwszy czynnik w postaci np. kodu PIN, ale nie zdobyła fizycznego klucza sprzętowego, nie będzie mogła autoryzować danej operacji. Jednakże jak wspominano wcześniej, taki klucz należy fizycznie mieć przy sobie w razie potrzeby, co dla części użytkowników może być uciążliwe. Również zgubienie czy utrata takiego klucza może spowodować niemały problem, ponieważ o ile użytkownik nie posiadał zapasowego klucza powiązanego z tymi samymi kontami, dostęp do nich może zostać utracony. Ten właśnie dodatkowy nakład pracy – czy to posiadanie klucza, przepisanie kodu lub wykonanie dodatkowych kroków – sprawia że autoryzacja wieloskładnikowa nie jest powszechnie wykorzystywana przez większość użytkowników, najczęściej na rzecz własnej wygody. W niektórych przypadkach aplikacje wymagają na korzystającym użycie dodatkowych czynników dla jego

bezpieczeństwa, co jest działaniem można powiedzieć ingerującym w jego decyzje, ale wielu z nich nawet nie zdaje sobie sprawy jak znacząco wzrasta poziom zabezpieczeń dzięki wykorzystaniu MFA.

3. Analiza SWOT/TOWS – teoretyczne podstawy

Zastosowana w niniejszej pracy metoda analizy SWOT/TOWS to popularna technika używana do oceny sytuacji strategicznej organizacji, produktu, usługi lub – jak ma to miejsce w tej pracy – systemu czy technologii. Analiza SWOT polega na identyfikacji wewnętrznych czynników pozytywnych i negatywnych, oraz czynników zewnętrznych – szans i zagrożeń – które mogą wpływać na dany obszar. Analiza TOWS jest natomiast rozszerzeniem metody SWOT i koncentruje się na badaniu od zewnątrz do wewnątrz, czyli obrazuje jak otoczenie zewnętrzne oddziałuje na przedmiot analizy [14].

Na składniki analizy SWOT składają się:

- Mocne strony (*Strengths*) – są to wewnętrzne zalety badanego przedmiotu, dające mu przewagę nad innymi. W przypadku metod autoryzacji mogą to być np. wygoda oferowana użytkownikowi lub wysoki poziom zabezpieczeń.
- Słabe strony (*Weaknesses*) – wewnętrzne wady analizowanego obiektu, które mogą osłabić jego skuteczność. Słabością metody autoryzacji może być przykładowo niska złożoność co czyni metodę bardziej podatną na ataki *brute force*.
- Szanse (*Opportunities*) – zewnętrzne trendy, które mogą korzystnie wpłynąć na przedmiot analizy. Przykładem jest rozwój technologii biometrycznych, który może poprawić szybkość metod które z nich korzystają.
- Zagrożenia (*Threats*) – to czynniki zewnętrzne negatywnie oddziałujące na skuteczność badanego obiektu. W kontekście autoryzacji zagrożeniem mogą być rozwijające się techniki ataków, które mogą pozwolić na obejście zaawansowanych zabezpieczeń

Analiza TOWS jako rozwinięcie metody SWOT pozwala na stworzenie strategii w oparciu o różne kombinacje czynników. Na podstawie zależności między tymi czynnikami można wskazać odpowiednią strategię dla przedmiotu analizy, którą wskazuje najwyższy iloczyn wag czynników oraz interakcji między nimi. Zarówno strategie jak i pytania na które odpowiada analiza TOWS zostaną przedstawione w drugiej części niniejszej pracy.

II. Część badawcza

Każdy z przedstawionych w poprzedniej części sposobów autoryzacji został poddany analizie zgodnie z techniką SWOT/TOWS, skupiającej się na mocnych i słabych stronach rozwiązań, a także ich szansach na korzystne zmiany oraz zagrożeniach mogących naruszyć ich bezpieczeństwo. Analiza ta miała na celu porównanie poziomu bezpieczeństwa danych metod i określenie ich podatności na ataki ze strony osób niepożądanych, oraz ocenę ich poziomu bezpieczeństwa.

4. Analiza metod autoryzacji

W rozdziale tym przeprowadzona zostanie analiza SWOT/TOWS względem każdej z wymienionych w tej pracy metod autoryzacji. W kontekście biznesowym ten rodzaj analizy prowadzi do wyłonienia odpowiedniej dla danego przedsiębiorstwa strategii [15], ale w celu dostosowania tej metody badawczej do kontekstu bezpieczeństwa informatycznego, opracowane zostały cztery strategie opisujące metody autoryzacji, które bazują na strategiach przedsiębiorstw:

- Strategia maxi-maxi – wykorzystanie mocnych stron danej metody autoryzacji w celu skorzystania z dostępnych szans na jej rozwój i udoskonalenie. Metoda taka charakteryzuje się wysokimi perspektywami na dalszy rozwój oraz zapewnia odpowiedni poziom zabezpieczeń dla użytkowników.
- Strategia maxi-mini – przewaga silnych stron towarzysząca niesprzyjającym warunkom zewnętrznym. Metoda oferuje wysoką skuteczność i mechanizmy bezpieczeństwa ale jest podatna na pewne zagrożenia. Istotne jest wykorzystanie jej atutów w celu minimalizacji podatności i utrzymania zaufania użytkowników.
- Strategia mini-maxi – metoda posiada słabe strony, podatności, braki, ale również i szanse których wykorzystanie może wyeliminować lub ograniczyć te słabości.
- Strategia mini-mini – niekorzystne czynniki zewnętrzne oraz liczne słabe punkty metody sugerują niski poziom bezpieczeństwa lub ewentualne zakończenie jej wspierania i wykorzystywania przez użytkowników.

Przed przystąpieniem do analizy wymagane jest zidentyfikowanie uwarunkowań wewnętrznych oraz zewnętrznych i oszacowanie ich wpływu na wybór strategii. Czynniki będą klasyfikowane w czterech podstawowych kategoriach: mocne strony, słabe strony, szanse oraz zagrożenia.

W celu określenia strategii dla każdej metody konieczne będzie odpowiedzenie na poniższy zestaw pytań, na które odpowiedzi zostaną zamieszczone w odpowiednich tabelach:

- Czy mocne strony metody pozwolą na wykorzystanie możliwych szans? (S-O)
- Czy mocne strony metody pomogą w pokonaniu zagrożeń? (S-T)
- Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans? (W-O)
- Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń? (W-T)
- Czy dostępne szanse zintensyfikują mocne strony metody? (O-S)
- Czy odkryte zagrożenia osłabią mocne strony? (T-S)
- Czy szanse pozwolą na przezwyciężenie słabych stron metody? (O-W)
- Czy ewentualne zagrożenia wzmocnią słabe strony? (T-W)

Po udzieleniu wszystkich odpowiedzi tabele zostaną podsumowane osobno dla analizy SWOT oraz TOWS i przedstawione zostanie zestawienie zbiorcze dla każdej metody, na podstawie którego możliwe będzie wyłonienie właściwej dla niej strategii.

4.1. Numeryczny kod PIN

Kod	Czynniki wewnętrzne		Kod	Czynniki zewnętrzne	
	Waga	Mocne strony		Waga	Szanse
S1	0.3	Prostota i łatwość użycia z perspektywy użytkownika	O1	0.45	Odpowiednio długi i skomplikowany kod PIN może być czasochłonny do złamania
S2	0.4	Uniwersalność i powszechna znajomość tej metody	O2	0.15	Technologie jak np. szkło prywatyzujące poprawiają bezpieczeństwo kodu PIN
S3	0.3	Szybkość dostępu	O3	0.4	Polityki wymuszające częstą zmianę kodu PIN
Kod	**Waga**	**Słabe strony**	**Kod**	**Waga**	**Zagrożenia**
W1	0.4	Podatność na ataki *brute force*	T1	0.2	Możliwość wykradzenia kodu PIN poprzez *phising, shoulder surfing*
W2	0.4	Możliwość odgadnięcia kodu przez znajomość użytkownika	T2	0.6	Wykorzystywanie prostych kodów
W3	0.2	Możliwość zapomnienia kodu PIN	T3	0.2	Rozwój mocy obliczeniowej komputerów pozwalający na szybsze łamanie kodu PIN

Tabela 4.1 Oszacowanie siły wpływu poszczególnych czynników na dobór strategii metody autoryzacji numerycznym kodem PIN - opracowanie własne

Mocne strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.3	0	0	2
S2	1	1	0	0.4	2	0,8	1
S3	0	0	0	0.3	0	0	2
Waga	0.45	0.15	0.4				
Liczba interakcji	1	1	0				
Iloczyn wag i interakcji	0,45	0,15	0				
Ranga	1	2	3				

Tabela 4.2 Identyfikacja interakcji mocnych stron i szans dla numerycznego kodu PIN – opracowanie własne

W tabeli 2.2 przedstawione zostały wyniki analizy interakcji pomiędzy mocnymi stronami i szansami omawianej metody. Z odpowiedzi na pytanie „Czy mocne strony metody pozwolą na wykorzystanie możliwych szans?" uzyskano sumę interakcji równą 2, stanowiącą 22% maksymalnej liczby interakcji w tym układzie. Łączna suma iloczynów wag i interakcji wynosiła natomiast 1.4.

Mocne strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.3	0	0	1
S2	0	0	0	0.4	0	0	1
S3	0	0	0	0.3	0	0	1
Waga	0.2	0.6	0.2				
Liczba interakcji	0	0	0				
Iloczyn wag i interakcji	0	0	0				
Ranga	1	1	1				

Tabela 4.3 Identyfikacja interakcji mocnych stron i zagrożeń dla Numerycznego kodu PIN - opracowanie własne

W tabeli 2.3 przedstawiono analizę interakcji odpowiadających na pytanie „Czy mocne strony metody pomogą w pokonaniu zagrożeń?”. Z powodu braku bezpośrednich interakcji między wymienionymi czynnikami, ich suma wyniosła 0, podobnie jak suma iloczynów wag i interakcji.

Słabe strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	0	0.4	0	0	2
W2	0	0	0	0.4	0	0	2
W3	1	0	1	0.2	2	0,4	1
Waga	0.45	0.15	0.4				
Liczba interakcji	1	0	1				
Iloczyn wag i interakcji	0,45	0	0,4				
Ranga	1	3	2				

Tabela 4.4 Identyfikacja interakcji słabych stron i szans dla numerycznego kodu PIN - opracowanie własne

Tabela 2.4 przedstawia odpowiedzi na pytanie „Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans?”. Po ich przeanalizowaniu można stwierdzić, że całkowita liczba interakcji w tym układzie wyniosła 2, co stanowi 22% maksymalnej sumy. Łączna suma iloczynów i wag interakcji jest równa w tym przypadku 1.35.

Słabe strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	1	1	0.4	2	0,8	1
W2	1	1	0	0.4	2	0,8	1
W3	0	0	0	0.2	0	0	2

Waga	0.2	0.6	0.2
Liczba interakcji	1	2	1
Iloczyn wag i interakcji	0,2	1,2	0,2
Ranga	2	1	2

Tabela 4.5 Identyfikacja interakcji słabych stron i zagrożeń dla numerycznego kodu PIN - opracowanie własne

Przedstawione odpowiedzi na pytanie „Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń?” w tabeli 2.5 pozwalają stwierdzić, że suma wszystkich interakcji wyniosła 4, uzyskując wynik 44% maksymalnej sumy interakcji, natomiast suma iloczynów wag i interakcji wyniosła 3.2.

Szanse/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	0	0	0	0.45	0	0	2
O2	1	0	0	0.15	1	0,15	1
O3	0	0	0	0.4	0	0	2
Waga	0.3	0.4	0.3				
Liczba interakcji	1	0	0				
Iloczyn wag i interakcji	0,3	0	0				
Ranga	1	2	2				

Tabela 4.6 Identyfikacja interakcji szans i mocnych stron dla numerycznego kodu PIN - opracowanie własne

Tabela 2.6 ukazuje odpowiedzi dotyczące pytania „Czy dostępne szanse zintensyfikują mocne strony metody?”. Suma wszystkich interakcji wyniosła 1, czyli 11% maksymalnego wyniku. Suma iloczynów wag i interakcji jest równa 0.45.

Zagrożenia/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	0	0	0.2	0	0	2
T2	1	0	0	0.6	1	0,6	1
T3	0	0	0	0.2	0	0	2
Waga	0.3	0.4	0.3				
Liczba interakcji	1	0	0				
Iloczyn wag i interakcji	0,3	0	0				
Ranga	1	2	2				

Tabela 4.7 Identyfikacja interakcji zagrożeń i mocnych stron dla numerycznego kodu PIN - opracowanie własne

Przedstawione w tabeli 2.7 wyniki będące odpowiedziami na pytanie „Czy odkryte zagrożenia osłabią mocne strony?" ukazują łączną liczbę interakcji w tym układzie równą 1, stanowiącą 11% maksymalnego wyniku, gdzie łączna suma iloczynów wag i interakcji równa jest 0.9.

Szanse/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	1	1	0	0.45	2	0,9	1
O2	0	1	0	0.15	1	0,15	3
O3	0	1	0	0.4	1	0,4	2
Waga	0.4	0.4	0.2				
Liczba interakcji	1	3	0				
Iloczyn wag i interakcji	0,4	1,2	0				
Ranga	2	1	3				

Tabela 4.8 Identyfikacja interakcji szans i słabych stron dla numerycznego kodu PIN - opracowanie własne

W tabeli 2.8 widoczne są interakcje czynników, na podstawie odpowiedzi na pytanie „Czy szanse pozwolą na przezwyciężenie słabych stron metody?”. Ich suma wyniosła 4, czyli 44% maksymalnej sumy w tej kombinacji. Suma wszystkich iloczynów wag i interakcji wyniosła 3.05.

Zagrożenia/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	1	0	0.2	1	0,2	2
T2	1	1	0	0.6	2	1,2	1
T3	1	0	0	0.2	1	0,2	2
Waga	0.4	0.4	0.2				
Liczba interakcji	2	2	0				
Iloczyn wag i interakcji	0,8	0,8	0				
Ranga	1	1	2				

Tabela 4.9 Identyfikacja interakcji zagrożeń i słabych stron dla numerycznego kodu PIN - opracowanie własne

Z tabeli 2.9 która zawiera odpowiedzi na pytanie „Czy ewentualne zagrożenia wzmocnią słabe strony?” można odczytać łączną sumę interakcji wynoszącą 4, będącą 44% maksymalnej możliwej sumy. W tej tabeli suma iloczynów wag i interakcji równa jest 3.2.

Kombinacja	Wynik analizy SWOT	
	Suma interakcji	Suma iloczynów
S/O	2	1.4
S/T	0	0
W/O	2	1.35
W/T	4	3.2

Tabela 4.10 Zestawienie zbiorcze wyników analizy SWOT dla numerycznego kodu PIN

Kombinacja	Wynik analizy TOWS	
	Suma interakcji	Suma iloczynów
O/S	1	0.45
T/S	1	0.9
O/W	4	3.05
T/W	4	3.2

Tabela 4.11 Zestawienie zbiorcze wyników analizy TOWS dla numerycznego kodu PIN

Na podstawie zbiorczych zestawień wyników analizy interakcji z tabel 2.10 oraz 2.11 możliwe jest dokonanie wyboru strategii dla metody autoryzacji numerycznym kodem PIN, co przedstawione zostało w tabeli 2.12.

Mocne strony [S]	**Szanse [O]**	**Zagrożenia [T]**
	Maxi-maxi	Maxi-mini
Suma interakcji	3	1
Suma iloczynów	1.85	0.9
Słabe strony [W]	Mini-maxi	Mini-mini
Suma interakcji	6	8
Suma iloczynów	4.4	6.4

Tabela 4.12 Wybór strategii na podstawie wyników analizy dla numerycznego kodu PIN

Jak widać w tabeli 2.12 dla metody autoryzacji numerycznym kodem PIN została wybrana strategia mini-mini. Świadczy to o przewadze słabych stron metody oraz niesprzyjających czynnikach zewnętrznych. W przypadku tej metody jej poziom bezpieczeństwa jest mocno uzależniony od zewnętrznych wymogów jak odpowiednia długość i złożoność kodu czy jego częste zmienianie. Niestety wskazania te nie są respektowane przez większość użytkowników, którzy dodatkowo stosują bardzo proste w odgadnięciu przez ludzi lub maszyny kombinacje. Autoryzacja numerycznym kodem PIN sama w sobie nie może więc zostać uznana za bezpieczną, jeżeli nie jest stosowana według dodatkowych warunków, które znacząco podnoszą poziom zaufania do niej, ale nie eliminują całkowicie jej podatności. Z tego też powodu kod PIN używany jest coraz częściej jako dodatkowy, kolejny składnik autoryzacji, w której główną rolę odgrywa inna, bezpieczniejsza metoda.

4.2. Silne i bezpieczne hasło

Kod	Czynniki wewnętrzne		Kod	Czynniki zewnętrzne	
	Waga	**Mocne strony**		**Waga**	**Szanse**
S1	0.2	Elastyczność pod kątem długości oraz znaków tworzących hasło	O1	0.3	Odpowiednio długie i skomplikowane hasło może być czasochłonne do złamania
S2	0.3	Uniwersalność i powszechna znajomość tej metody	O2	0.4	Menadżery haseł ułatwiają przechowywanie skomplikowanych haseł
S3	0.5	Zwiększenie bezpieczeństwa hasła poprzez np. haszowanie	O3	0.3	Polityki wymuszające odpowiednią złożoność haseł
Kod	**Waga**	**Słabe strony**	**Kod**	**Waga**	**Zagrożenia**
W1	0.4	Podatność na ataki *brute force*	T1	0.2	Możliwość wykradzenia hasła poprzez *phising, shoulder surfing*
W2	0.3	Możliwość odgadnięcia hasła przez znajomość użytkownika	T2	0.6	Wykorzystywanie prostych haseł
W3	0.3	Możliwość zapomnienia zbyt długiego czy skomplikowanego hasła	T3	0.2	Rozwój mocy obliczeniowej komputerów pozwalający na szybsze łamanie haseł

Tabela 4.13 Oszacowanie siły wpływu poszczególnych czynników na dobór strategii metody autoryzacji hasłem - opracowanie własne

Mocne strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga

S1	1	1	1	0.2	3	0,6	1
S2	0	0	0	0.3	0	0	3
S3	1	0	0	0.5	1	0,5	2
Waga	0.3	0.4	0.3				
Liczba interakcji	2	1	1				
Iloczyn wag i interakcji	0,6	0,4	0,3				
Ranga	1	2	3				

Tabela 4.14 Identyfikacja interakcji mocnych stron i szans dla hasła – opracowanie własne

W tabeli 2.14 widoczne są interakcje pomiędzy mocnymi stronami i szansami omawianej metody. Odpowiedzi na pytanie „Czy mocne strony metody pozwolą na wykorzystanie możliwych szans?" dały sumę interakcji równą 4, będącą 44% maksymalnej liczby interakcji tego układu. Łączna suma iloczynów wag i interakcji wyniosła 2.4.

Mocne strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	1	1	0.2	2	0,4	2
S2	0	0	0	0.3	0	0	3
S3	0	0	1	0.5	1	0,5	1
Waga	0.2	0.6	0.2				
Liczba interakcji	0	1	2				
Iloczyn wag i interakcji	0	0,6	0,4				
Ranga	3	1	2				

Tabela 4.15 Identyfikacja interakcji mocnych stron i zagrożeń dla hasła- opracowanie własne

W tabeli 2.15 ukazano analizę interakcji odpowiadających na pytanie „Czy mocne strony metody pomogą w pokonaniu zagrożeń?". Suma wszystkich interakcji wyniosła w

tym przypadku 3, co stanowi 33% maksymalnego wyniku, a suma iloczynów wag i interakcji jest równa 1.9.

Słabe strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	0	0.4	0	0	2
W2	0	0	0	0.3	0	0	2
W3	1	0	1	0.3	2	0,6	1
Waga	0.3	0.4	0.3				
Liczba interakcji	1	0	1				
Iloczyn wag i interakcji	0,3	0	0,3				
Ranga	1	2	1				

Tabela 4.16 Identyfikacja interakcji słabych stron i szans dla hasła - opracowanie własne

Tabela 2.16 obrazuje odpowiedzi na pytanie „Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans?”. Podsumowując, całkowita liczba interakcji w tym układzie wyniosła 2, co stanowi 22% maksymalnej sumy. Suma iloczynów i wag interakcji jest równa w tym przypadku 1.2.

Słabe strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	1	1	0.4	2	0,8	1
W2	1	1	0	0.3	2	0,6	2
W3	0	0	0	0.3	0	0	3
Waga	0.2	0.6	0.2				
Liczba interakcji	1	2	1				

Iloczyn wag i interakcji	0,2	1,2	0,2
Ranga	2	1	2

Tabela 4.17 Identyfikacja interakcji słabych stron i zagrożeń dla hasła - opracowanie własne

Odpowiedzi na pytanie „Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń?” z tabeli 2.17 ukazują, że suma wszystkich interakcji wyniosła 4, co daje 44% maksymalnej sumy interakcji, a suma iloczynów wag i interakcji wyniosła 3.

Szanse/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	1	0	1	0.3	2	0,6	1
O2	1	0	0	0.4	1	0,4	2
O3	1	0	1	0.3	2	0,6	1
Waga	0.2	0.3	0.5				
Liczba interakcji	3	0	2				
Iloczyn wag i interakcji	0,6	0	1				
Ranga	2	3	1				

Tabela 4.18 Identyfikacja interakcji szans i mocnych stron dla hasła - opracowanie własne

Tabela 2.18 przedstawia odpowiedzi dotyczące pytania „Czy dostępne szanse zintensyfikują mocne strony metody?”. Suma interakcji wyniosła 5, czyli 55% maksymalnego wyniku. Suma iloczynów wag i interakcji jest równa 3.2.

Zagrożenia/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	0	0	0.2	0	0	3

T2	1	0	1	0.6	2	1,2	1
T3	0	0	1	0.2	1	0,2	2
Waga	0.2	0.3	0.5				
Liczba interakcji	1	0	2				
Iloczyn wag i interakcji	0,2	0	1				
Ranga	2	3	1				

Tabela 4.19 Identyfikacja interakcji zagrożeń i mocnych stron dla hasła - opracowanie własne

Przedstawione w tabeli 2.19 wyniki odpowiadające na pytanie „Czy odkryte zagrożenia osłabią mocne strony?" ukazują łączną liczbę interakcji w tym układzie równą 3, stanowiącą 33% maksymalnego wyniku, z łączną sumą iloczynów wag i interakcji równą 2.6.

Szanse/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	1	0	0	0.3	1	0,3	2
O2	0	0	1	0.4	1	0,4	1
O3	1	0	0	0.3	1	0,3	2
Waga	0.4	0.3	0.3				
Liczba interakcji	2	0	1				
Iloczyn wag i interakcji	0,8	0	0,3				
Ranga	1	3	2				

Tabela 4.20 Identyfikacja interakcji szans i słabych stron dla hasła - opracowanie własne

W tabeli 2.20 widoczne są interakcje odpowiadające na pytanie „Czy szanse pozwolą na przezwyciężenie słabych stron metody?". Ich suma wyniosła 3, czyli 33% maksymalnej sumy. Suma wszystkich iloczynów wag i interakcji wyniosła 3.1.

Zagrożenia/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	1	0	0.2	1	0,2	2
T2	1	1	0	0.6	2	1,2	1
T3	1	0	0	0.2	1	0,2	2
Waga	0.4	0.3	0.3				
Liczba interakcji	2	2	0				
Iloczyn wag i interakcji	0,8	0,6	0				
Ranga	1	2	3				

Tabela 4.21 Identyfikacja interakcji zagrożeń i słabych stron dla hasła - opracowanie własne

Tabela 2.21 zawiera odpowiedzi na pytanie „Czy ewentualne zagrożenia wzmocnią słabe strony?" gdzie łączna suma interakcji wynosi 4 i stanowi 44% maksymalnej możliwej sumy. W tej tabeli suma iloczynów wag i interakcji równa jest 3.

Kombinacja	Wynik analizy SWOT	
	Suma interakcji	Suma iloczynów
S/O	4	2.4
S/T	3	1.9
W/O	2	1.2
W/T	4	3

Tabela 4.22 Zestawienie zbiorcze wyników analizy SWOT dla hasła

Kombinacja	Wynik analizy TOWS	
	Suma interakcji	Suma iloczynów
O/S	5	3.2
T/S	3	2.6
O/W	3	3.1
T/W	4	3

Tabela 4.23 Zestawienie zbiorcze wyników analizy TOWS dla hasła

Na podstawie zbiorczych zestawień wyników analizy interakcji z tabel 2.22 oraz 2.23 można określić strategię dla metody autoryzacji hasłem, co przedstawione zostało w tabeli 2.24.

Mocne strony [S]	**Szanse [O]**	**Zagrożenia [T]**
	Maxi-maxi	Maxi-mini
Suma interakcji	9	6
Suma iloczynów	5.6	4.5
Słabe strony [W]	Mini-maxi	Mini-mini
Suma interakcji	5	8
Suma iloczynów	4.3	6

Tabela 4.24 Wybór strategii na podstawie wyników analizy dla hasła

W tabeli 2.24 można zauważyć, że dla metody autoryzacji hasłem została wybrana strategia mini-mini, dla której uzyskana została największa suma iloczynów. Jest to ta sama strategia jak w przypadku numerycznego kodu PIN. Bezpieczeństwo tej metody, podobnie jak wcześniej omawianej, jest mocno uwarunkowane zewnętrznymi czynnikami które nakładają na nią pewne wymogi mające na celu podnieść jej poziom zabezpieczeń. Metoda ta z całą pewnością posiada dużą ilość słabych stron, ale warto zauważyć że analiza pokazuje niewielką różnicę w stosunku do strategii maxi-maxi, z uwagi na wiele zewnętrznych czynników które dostosowują tą metodę do odpowiednich sposobów wykorzystania. Jednakże bez tych czynników metoda nie wykazuje się wystarczająco wysokim poziomem bezpieczeństwa i nie można jej uznać za taką samą w sobie. Metoda autoryzacji hasłem z uwagi na ogromną popularność oraz uniwersalność z całą pewnością nie zostanie prędko całkowicie wyparta przez inne, ale stosowanie jej bez odpowiednich polityk bezpieczeństwa jest niewystarczające dla zapewnienia odpowiedniego poziomu ochrony.

4.3. Rysowanie wzoru na ekranie

Kod	Czynniki wewnętrzne		Kod	Czynniki zewnętrzne	
	Waga	Mocne strony		Waga	Szanse
S1	0.4	Intuicyjność i łatwość zapamiętania	O1	0.2	Powierzchnie ekranów niwelujące ślady palców, co utrudnia odczytanie wzoru
S2	0.4	Szybkość i wygoda użycia	O2	0.4	Umożliwienie rozszerzenia siatki pól, co znacząco zwiększa złożoność wzoru
S3	0.2	Potrzeba specjalistycznego oprogramowania symulującego dotknięcia aby łamać wzór przy użyciu maszyny	O3	0.4	Polityka wymuszająca częstą zmianę wzoru
Kod	**Waga**	**Słabe strony**	**Kod**	**Waga**	**Zagrożenia**
W1	0.1	Podatność na ataki *brute force*	T1	0.3	Możliwość wykradzenia hasła poprzez *shoulder surfing*
W2	0.5	Ślady palców na ekranie przy częstym wprowadzaniu wzoru mogą go ujawnić	T2	0.4	Wykorzystywanie prostych wzorów
W3	0.4	Ograniczona złożoność wzoru przez limit jego długości	T3	0.3	Brak polityk wymuszających odpowiednio skomplikowany wzór

Tabela 4.25 Oszacowanie siły wpływu poszczególnych czynników na dobór strategii metody autoryzacji wzorem - opracowanie własne

Mocne strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	1	0	0.4	1	0,4	1
S2	0	0	0	0.4	0	0	2
S3	0	0	0	0.2	0	0	2
Waga	0.2	0.4	0.4				
Liczba interakcji	0	1	0				
Iloczyn wag i interakcji	0	0,4	0				
Ranga	2	1	2				

Tabela 4.26 Identyfikacja interakcji mocnych stron i szans dla wzoru – opracowanie własne

W tabeli 2.26 przedstawione są interakcje pomiędzy mocnymi stronami i szansami omawianej metody. Odpowiedzi na pytanie „Czy mocne strony metody pozwolą na wykorzystanie możliwych szans?" uzyskały sumę interakcji równą 1, dającą 11% maksymalnej liczby interakcji tego układu. Łączna suma iloczynów wag i interakcji wyniosła 0.8.

Mocne strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.4	0	0	1
S2	0	0	0	0.4	0	0	1
S3	0	0	0	0.2	0	0	1
Waga	0.3	0.4	0.3				
Liczba interakcji	0	0	0				
Iloczyn wag i interakcji	0	0	0				
Ranga	1	1	1				

Tabela 4.27 Identyfikacja interakcji mocnych stron i zagrożeń dla wzoru- opracowanie własne

W tabeli 2.27 przeprowadzono analizę interakcji odpowiadających na pytanie „Czy mocne strony metody pomogą w pokonaniu zagrożeń?”. W tym przypadku suma wszystkich interakcji wyniosła 0, podobnie jak suma iloczynów.

Słabe strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	0	0.1	0	0	2
W2	0	1	1	0.5	2	1	1
W3	0	0	0	0.4	0	0	2
Waga	0.2	0.4	0.4				
Liczba interakcji	0	1	1				
Iloczyn wag i interakcji	0	0,4	0,4				
Ranga	2	1	1				

Tabela 4.28 Identyfikacja interakcji słabych stron i szans dla wzoru - opracowanie własne

Tabela 2.28 przedstawia odpowiedzi na pytanie „Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans?”. Suma interakcji w tym układzie wyniosła 2, co daje 22% maksymalnej sumy. Suma iloczynów i wag interakcji jest równa w tym przypadku 1.8.

Słabe strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	1	0	0.1	1	0,1	3
W2	1	0	0	0.5	1	0,5	1
W3	0	1	0	0.4	1	0,4	2
Waga	0.2	0.4	0.4				
Liczba interakcji	1	2	0				

Iloczyn wag i interakcji	0,2	0,8	0
Ranga	2	1	3

Tabela 4.29 Identyfikacja interakcji słabych stron i zagrożeń dla wzoru - opracowanie własne

Odpowiedzi na pytanie „Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń?” z tabeli 2.29 dają łączną liczbę wszystkich interakcji równą 3, co daje 33% maksymalnej sumy interakcji, a suma iloczynów wag i interakcji wyniosła 2.

Szanse/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	0	0	0	0.2	0	0	1
O2	1	0	1	0.4	2	0,8	2
O3	0	0	1	0.4	1	0,4	1
Waga	0.4	0.4	0.2				
Liczba interakcji	1	0	2				
Iloczyn wag i interakcji	0,4	0	0,4				
Ranga	2	3	1				

Tabela 4.30 Identyfikacja interakcji szans i mocnych stron dla wzoru - opracowanie własne

Tabela 2.30 opisuje odpowiedzi na pytanie „Czy dostępne szanse zintensyfikują mocne strony metody?”. Suma interakcji osiągnęła w tym przypadku wynik 3, stanowiący 33% maksymalnego. Suma iloczynów wag i interakcji wynosi 2.

Zagrożenia/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	0	0	0.3	0	0	3

T2	1	0	1	0.4	2	0,8	1
T3	1	0	1	0.3	2	0,6	2
Waga	0.4	0.4	0.2				
Liczba interakcji	2	0	2				
Iloczyn wag i interakcji	0,8	0	0,4				
Ranga	1	3	2				

Tabela 4.31 Identyfikacja interakcji zagrożeń i mocnych stron dla wzoru - opracowanie własne

Przedstawione w tabeli 2.31 wyniki odpowiadające na pytanie „Czy odkryte zagrożenia osłabią mocne strony?" przedstawiają łączną liczbę interakcji w tym układzie wynoszącą 4, stanowiącą 44% maksymalnego wyniku, z łączną sumą iloczynów wag i interakcji równą 2.4.

Szanse/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	0	1	0	0.2	1	0,2	2
O2	1	0	1	0.4	2	0,8	1
O3	0	0	0	0.4	0	0	3
Waga	0.1	0.5	0.4				
Liczba interakcji	1	1	1				
Iloczyn wag i interakcji	0,1	0,5	0,4				
Ranga	3	1	2				

Tabela 4.32 Identyfikacja interakcji szans i słabych stron dla wzoru - opracowanie własne

W tabeli 2.32 przedstawione są interakcje odpowiadające na pytanie „Czy szanse pozwolą na przezwyciężenie słabych stron metody?". Suma wyniosła 3, czyli 33% maksymalnej sumy. Suma wszystkich iloczynów wag i interakcji wyniosła 2.

Zagrożenia/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	1	0	0.3	1	0,3	2
T2	1	0	0	0.4	1	0,4	1
T3	1	0	0	0.3	1	0,3	2
Waga	0.1	0.5	0.4				
Liczba interakcji	2	1	0				
Iloczyn wag i interakcji	0,2	0,5	0				
Ranga	1	2	3				

Tabela 4.33 Identyfikacja interakcji zagrożeń i słabych stron dla wzoru - opracowanie własne

Tabela 2.33 zawiera odpowiedzi na pytanie „Czy ewentualne zagrożenia wzmocnią słabe strony?”, łączna suma interakcji wynosi 3 i jest to 33% maksymalnej możliwej sumy. W tej konfiguracji suma iloczynów wag i interakcji równa jest 1.7.

Kombinacja	Wynik analizy SWOT	
	Suma interakcji	Suma iloczynów
S/O	1	0.8
S/T	0	0
W/O	2	1.8
W/T	3	2

Tabela 4.34 Zestawienie zbiorcze wyników analizy SWOT dla wzoru

Kombinacja	Wynik analizy TOWS	
	Suma interakcji	Suma iloczynów
O/S	3	2
T/S	4	2.4
O/W	3	2
T/W	3	1.7

Tabela 4.35 Zestawienie zbiorcze wyników analizy TOWS dla wzoru

Na podstawie zbiorczych zestawień wyników analizy interakcji z tabel 2.34 oraz 2.35 można ustalić strategię dla metody autoryzacji wzorem, co przedstawione zostało w tabeli 2.36.

Mocne strony [S]	**Szanse [O]**	**Zagrożenia [T]**
	Maxi-maxi	Maxi-mini
Suma interakcji	4	4
Suma iloczynów	2.8	2.4
Słabe strony [W]	Mini-maxi	Mini-mini
Suma interakcji	5	6
Suma iloczynów	3.8	3.7

Tabela 4.36 Wybór strategii na podstawie wyników analizy dla wzoru

W tabeli 2.36 widać, że dla metody autoryzacji wzorem została określona strategia mini-maxi, dla której uzyskana została największa suma iloczynów. Można więc stwierdzić, że w przypadku tej metody przeważa liczba dostępnych dla niej szans ale także i jej słabych stron. Powinno dążyć się do wykorzystania tychże szans w celu wyeliminowania jej słabych stron, jak np. można zniwelować problem ograniczonej złożoności poprzez udostępnienie możliwości rozszerzenia siatki dostępnych pól. Autoryzacja wzorem, podobnie jak poprzednie metody, sama w sobie nie oferuje wystarczającego poziomu zabezpieczeń i najlepiej aby była stosowana razem z odpowiednimi, zewnętrznymi czynnikami. Dzięki szerokiemu wachlarzowi dostępnych szans metoda ta ma możliwość jeszcze długo utrzymać się na urządzeniach konsumenckich, lecz istotne jest aby producenci zarówno oprogramowania jak i urządzeń zadbali o jej odpowiednie dostosowanie, mając na uwadze jej ograniczenia i słabości.

4.4. Rozpoznawanie twarzy (Face unlock)

Kod	Czynniki wewnętrzne		Kod	Czynniki zewnętrzne	
	Waga	Mocne strony		Waga	Szanse
S1	0.5	Wygoda, brak konieczności pamiętania czegokolwiek	O1	0.4	Integracja z dodatkowymi czynnikami jak rozpoznawanie głosu, co zwiększa bezpieczeństwo metody
S2	0.3	Zaawansowane systemy rozpoznawania bazujące na podczerwieni lub obrazie 3D	O2	0.4	Aktywny rozwój tej technologii mający na celu zniwelowanie problemu złego oświetlenia i polepszenia algorytmów identyfikujących twarz
S3	0.2	Trudna w złamaniu poprzez symulowanie twarzy użytkownika – wymaga specjalistycznego oprogramowania	O3	0.2	Polityki chroniące dane biometryczne użytkownika zwiększające zaufanie do metody
Kod	**Waga**	**Słabe strony**	**Kod**	**Waga**	**Zagrożenia**
W1	0.3	Narażenie prywatności użytkownika poprzez przechowywanie danych o jego twarzy	T1	0.3	W niekorzystnych warunkach oświetleniowych wykorzystanie metody jest utrudnione
W2	0.3	Bardziej zaawansowane technologie identyfikacji twarzy wymagają specjalnych sensorów co zwiększa koszt wdrożenia	T2	0.5	Wykorzystanie sztucznej inteligencji do tworzenia *deepfake'ów* mających na celu oszukanie tej metody

W3	0.4	Mniej zaawansowane systemy da się oszukać zdjęciem lub nagraniem twarzy użytkownika	T3	0.2	Możliwość nadużycia lub wykradnięcia danych dotyczących twarzy użytkownika

Tabela 4.37 Oszacowanie siły wpływu poszczególnych czynników na dobór strategii metody autoryzacji twarzą - opracowanie własne

Mocne strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	1	0	0	0.5	1	0,5	1
S2	0	1	0	0.3	1	0,3	3
S3	1	1	0	0.2	2	0,4	2
Waga	0.4	0.4	0.2				
Liczba interakcji	2	2	0				
Iloczyn wag i interakcji	0,8	0,8	0				
Ranga	1	1	2				

Tabela 4.38 Identyfikacja interakcji mocnych stron i szans dla autoryzacji twarzą – opracowanie własne

W tabeli 2.38 ukazane są interakcje pomiędzy mocnymi stronami i szansami omawianej metody. Odpowiedzi na pytanie „Czy mocne strony metody pozwolą na wykorzystanie możliwych szans?” otrzymały sumę interakcji wynoszącą 4, dającą 44% maksymalnej liczby interakcji w tym układzie. Łączna suma iloczynów wag i interakcji wyniosła 2.8.

Mocne strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.5	0	0	3

S2	1	1	0	0.3	2	0,6	1
S3	0	1	0	0.2	1	0,2	2
Waga	0.3	0.5	0.2				
Liczba interakcji	1	2	0				
Iloczyn wag i interakcji	0,3	1	0				
Ranga	2	1	3				

Tabela 4.39 Identyfikacja interakcji mocnych stron i zagrożeń dla autoryzacji twarzą- opracowanie własne

W tabeli 2.39 widać analizę interakcji odpowiadających na pytanie „Czy mocne strony metody pomogą w pokonaniu zagrożeń?”. W tym przypadku suma wszystkich interakcji wyniosła 3, a suma iloczynów 2.1.

Słabe strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	1	0.3	1	0,3	2
W2	1	1	0	0.3	2	0,6	1
W3	0	0	0	0.4	0	0	3
Waga	0.4	0.4	0.2				
Liczba interakcji	1	1	1				
Iloczyn wag i interakcji	0,4	0,4	0,2				
Ranga	1	1	2				

Tabela 4.40 Identyfikacja interakcji słabych stron i szans dla autoryzacji twarzą - opracowanie własne

Tabela 2.40 przedstawia odpowiedzi na pytanie „Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans?”. Suma interakcji w tym przypadku wyniosła 3, co daje 33% maksymalnej sumy tego układu. Suma iloczynów i wag interakcji wyniosła natomiast 1.9.

Słabe strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	1	0.3	1	0,3	2
W2	0	0	0	0.3	0	0	3
W3	0	1	0	0.4	1	0,4	1
Waga	0.3	0.5	0.2				
Liczba interakcji	0	1	1				
Iloczyn wag i interakcji	0	0,5	0,2				
Ranga	3	1	2				

Tabela 4.41 Identyfikacja interakcji słabych stron i zagrożeń dla autoryzacji twarzą - opracowanie własne

Odpowiedzi na pytanie „Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń?" z tabeli 2.41 uzyskały łączną liczbę wszystkich interakcji równą 2, co stanowi 22% maksymalnej sumy interakcji, a suma iloczynów wag i interakcji osiągnęła wynik 1.4.

Szanse/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	1	0	1	0.4	2	0,8	1
O2	0	1	1	0.4	2	0,8	1
O3	0	0	0	0.2	0	0	2
Waga	0.5	0.3	0.2				
Liczba interakcji	1	1	2				
Iloczyn wag i interakcji	0,5	0,3	0,4				
Ranga	1	3	2				

Tabela 4.42 Identyfikacja interakcji szans i mocnych stron dla autoryzacji twarzą - opracowanie własne

Tabela 2.42 przedstawia odpowiedzi na pytanie „Czy dostępne szanse zintensyfikują mocne strony metody?”. W tym przypadku suma interakcji wynosi 4, co stanowi 44% maksymalnego wyniku. Suma iloczynów wag i interakcji wynosi natomiast 2.8.

Zagrożenia/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	1	0	0	0.3	1	0,3	2
T2	0	1	1	0.5	2	1	1
T3	0	0	0	0.2	0	0	3
Waga	0.5	0.3	0.2				
Liczba interakcji	1	1	1				
Iloczyn wag i interakcji	0,5	0,3	0,2				
Ranga	1	2	3				

Tabela 4.43 Identyfikacja interakcji zagrożeń i mocnych stron dla autoryzacji twarzą - opracowanie własne

Przedstawione w tabeli 2.43 wyniki odpowiadające na pytanie „Czy odkryte zagrożenia osłabią mocne strony?” ukazują łączną liczbę interakcji w tym układzie w liczbie 3, stanowiącą 33% maksymalnego wyniku, oraz łączną sumą iloczynów wag i interakcji równą 2.3.

Szanse/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	0	0	1	0.4	1	0,4	1
O2	0	0	1	0.4	1	0,4	1
O3	1	0	0	0.2	1	0,2	2
Waga	0.3	0.3	0.4				
Liczba interakcji	1	0	2				

Iloczyn wag i interakcji	0,3	0	0,8
Ranga	2	3	1

Tabela 4.44 Identyfikacja interakcji szans i słabych stron dla autoryzacji twarzą - opracowanie własne

W tabeli 2.44 przedstawione są interakcje odpowiadające na pytanie „Czy szanse pozwolą na przezwyciężenie słabych stron metody?”. Suma ich wyniosła 3, co daje 33% maksymalnej sumy. Suma wszystkich iloczynów wag i interakcji równa jest 2.1.

Zagrożenia/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	0	0	0.3	0	0	3
T2	0	0	1	0.5	1	0,5	1
T3	1	0	0	0.2	1	0,2	2
Waga	0.3	0.3	0.4				
Liczba interakcji	1	0	1				
Iloczyn wag i interakcji	0,3	0	0,4				
Ranga	2	3	1				

Tabela 4.45 Identyfikacja interakcji zagrożeń i słabych stron dla autoryzacji twarzą - opracowanie własne

Tabela 2.45 przedstawia odpowiedzi na pytanie „Czy ewentualne zagrożenia wzmocnią słabe strony?”, gdzie łączna suma interakcji wynosi 2 i stanowi 22% maksymalnego wyniku. W tej konfiguracji suma iloczynów wag i interakcji wyniosła 1.4.

Kombinacja	Wynik analizy SWOT	
	Suma interakcji	Suma iloczynów
S/O	4	2.8
S/T	3	2.1
W/O	3	1.9

W/T	2	1.4

Tabela 4.46 Zestawienie zbiorcze wyników analizy SWOT dla autoryzacji twarzą

Kombinacja	Wynik analizy TOWS	
	Suma interakcji	Suma iloczynów
O/S	4	2.8
T/S	3	2.3
O/W	3	2.1
T/W	2	1.4

Tabela 4.47 Zestawienie zbiorcze wyników analizy TOWS dla autoryzacji twarzą

Na podstawie zbiorczych zestawień wyników analizy interakcji z tabel 2.46 oraz 2.47 można ustalić strategię dla metody autoryzacji twarzą, co przedstawione zostało w tabeli 2.48.

Mocne strony [S]	**Szanse [O]**	**Zagrożenia [T]**
	Maxi-maxi	Maxi-mini
Suma interakcji	8	6
Suma iloczynów	5.6	4.4
Słabe strony [W]	Mini-maxi	Mini-mini
Suma interakcji	6	4
Suma iloczynów	4	2.8

Tabela 4.48 Wybór strategii na podstawie wyników analizy dla autoryzacji twarzą

W tabeli 2.48 można zauważyć, że w przypadku metody autoryzacji twarzą wybrana została strategia maxi-maxi co świadczy o dużej ilości szans wokół niej oraz silnych, pozytywnych cechach. Dla tej metody istotne jest więc aby aktywnie dążono do wykorzystania potencjalnych okazji jak np. integracja z innymi rodzajami metod typu rozpoznawanie głosu, w celu rozszerzenia jej wykorzystania o nowe zastosowania. Warto zwrócić uwagę że jest to pierwsza z omawianych metod, która wykorzystuje wrażliwe dane użytkownika, ale w większości przypadków korzystający z tej metody akceptują naruszenie swojej prywatności na rzecz wygody oferowanej przez nią. Metoda autoryzacji twarzą jest aktywnie rozwijana, a dzięki wykorzystaniu coraz to

nowszych i bardziej zaawansowanych sensorów podnoszony jest zapewniany przez nią poziom bezpieczeństwa. Istotnym faktem jednak jest to, że niewielu producentów telefonów z systemem Android decyduje się na implementację tejże metody autoryzacji – jest ona głównie spotykana w technologii FaceID oferowanej przez system IOS firmy Apple. Być może jest to spowodowane wspomnianym wyższym kosztem rozwoju i wprowadzenia do urządzeń, lub faktem, że nie jest to najpopularniej wykorzystywana metoda wśród użytkowników.

4.5. Znana lokalizacja, pobliskie urządzenia i kontakt z ciałem

Kod	Czynniki wewnętrzne		Kod	Czynniki zewnętrzne	
	Waga	Mocne strony		Waga	Szanse
S1	0.4	Wygoda i szybkość dzięki automatyzacji procesu	O1	0.4	Zwiększenie precyzji określania lokalizacji z użyciem zaawansowanych satelitów GPS
S2	0.3	Elastyczność, możliwość dobrania do użytkownika preferowanego sposobu odblokowania	O2	0.4	Rozwój technologii IoT może zapewnić nowe urządzenia pełniące rolę „klucza” do telefonu
S3	0.3	Znane urządzenia lub lokalizacja pełnią rolę dodatkowego czynnika, zwiększając bezpieczeństwo	O3	0.2	Możliwość personalizacji metody poprzez czasowe ograniczenia działania lub dynamiczne znane lokalizacje
Kod	**Waga**	**Słabe strony**	**Kod**	**Waga**	**Zagrożenia**
W1	0.4	Smart Lock może się pomylić (zwłaszcza jeśli chodzi o kontakt z ciałem) i omyłkowo odblokować urządzenie kiedy posiada je inna osoba	T1	0.3	Urządzenie może zostać odblokowane jeśli osoba trzecia zna zaufaną lokalizację lub pozyska zaufane urządzenie
W2	0.3	Odblokowanie w określonej lokalizacji jest ryzykowne, gdyż nie weryfikuje tożsamości osoby	T2	0.6	Niewłaściwe korzystanie z metody przez użytkowników, tj. ustawianie zaufanej lokalizacji w miejscach

					publicznych i pozostawianie urządzeń bez nadzoru
W3	0.3	Dopóki zaufane urządzenie jest w zasięgu to telefon może zostać odblokowany, nawet jeśli urządzenia są np. w różnych pomieszczeniach	T3	0.1	Ataki na urządzenie polegające na manipulacji danymi GPS lub podszywaniu się pod zaufane urządzenie

Tabela 4.49 Oszacowanie siły wpływu poszczególnych czynników na dobór strategii metody Smart Lock - opracowanie własne

Mocne strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.4	0	0	2
S2	0	1	1	0.3	2	0,6	1
S3	1	1	0	0.3	2	0,6	1
Waga	0.4	0.4	0.2				
Liczba interakcji	1	2	1				
Iloczyn wag i interakcji	0,4	0,8	0,2				
Ranga	2	1	3				

Tabela 4.50 Identyfikacja interakcji mocnych stron i szans dla metody Smart Lock – opracowanie własne

W tabeli 2.50 widoczne są interakcje pomiędzy mocnymi stronami i szansami omawianej metody. Odpowiedzi na pytanie „Czy mocne strony metody pozwolą na wykorzystanie możliwych szans?” uzyskały sumę interakcji wynoszącą 4, dającą 44% maksymalnej liczby interakcji w tym układzie, a łączna suma iloczynów wag i interakcji wyniosła 2.6.

Mocne strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.4	0	0	1
S2	0	0	0	0.3	0	0	1
S3	0	0	0	0.3	0	0	1
Waga	0.3	0.6	0.1				
Liczba interakcji	0	0	0				
Iloczyn wag i interakcji	0	0	0				
Ranga	1	1	1				

Tabela 4.51 Identyfikacja interakcji mocnych stron i zagrożeń dla metody Smart Lock - opracowanie własne

W tabeli 2.51 przedstawiono analizę interakcji będących odpowiedziami na pytanie „Czy mocne strony metody pomogą w pokonaniu zagrożeń?”. Suma wszystkich interakcji wyniosła 0, jak również suma iloczynów.

Słabe strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	0	0.4	0	0	2
W2	1	0	1	0.3	2	0,6	1
W3	0	1	1	0.3	2	0,6	1
Waga	0.4	0.4	0.2				
Liczba interakcji	1	1	2				
Iloczyn wag i interakcji	0,4	0,4	0,4				
Ranga	1	1	1				

Tabela 4.52 Identyfikacja interakcji słabych stron i szans dla metody Smart Lock - opracowanie własne

Tabela 2.52 obrazuje odpowiedzi na pytanie „Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans?”. Suma interakcji w tej sytuacji wyniosła 4, co daje 44% maksymalnej sumy tego układu. Suma iloczynów i wag interakcji równa jest 2.4.

Słabe strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	1	0	0.4	1	0,4	2
W2	1	1	1	0.3	3	0,9	1
W3	1	1	1	0.3	3	0,9	1
Waga	0.3	0.6	0.1				
Liczba interakcji	2	3	2				
Iloczyn wag i interakcji	0,6	1,8	0,2				
Ranga	2	1	3				

Tabela 4.53 Identyfikacja interakcji słabych stron i zagrożeń dla metody Smart Lock - opracowanie własne

Odpowiedzi na pytanie „Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń?” przedstawione w tabeli 2.53 osiągnęły łączną liczbę wszystkich interakcji dającą 7, co stanowi 77% maksymalnej sumy interakcji. Suma iloczynów wag i interakcji dała wynik 4.8.

Szanse/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	1	0	1	0.4	2	0,8	2
O2	1	1	1	0.4	3	1,2	1
O3	1	1	0	0.2	2	0,4	3
Waga	0.4	0.3	0.3				

Liczba interakcji	3	2	2
Iloczyn wag i interakcji	1,2	0,6	0,6
Ranga	1	2	2

Tabela 4.54 Identyfikacja interakcji szans i mocnych stron dla metody Smart Lock - opracowanie własne

Tabela 2.54 ukazuje odpowiedzi na pytanie „Czy dostępne szanse zintensyfikują mocne strony metody?”. W tym przykładzie suma interakcji wyniosła 7, co stanowi 77% maksymalnego wyniku. Suma iloczynów wag i interakcji równa jest natomiast 4.8.

Zagrożenia/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	1	0	1	0.3	2	0,6	2
T2	1	0	1	0.6	2	1,2	1
T3	1	0	1	0.1	2	0,2	3
Waga	0.4	0.3	0.3				
Liczba interakcji	3	0	3				
Iloczyn wag i interakcji	1,2	0	0,9				
Ranga	1	3	2				

Tabela 4.55 Identyfikacja interakcji zagrożeń i mocnych stron dla metody Smart Lock - opracowanie własne

Widoczne w tabeli 2.55 wyniki odpowiadające na pytanie „Czy odkryte zagrożenia osłabią mocne strony?” dają łączną liczbę interakcji równą 6, stanowiącą 66% maksymalnego wyniku, oraz całkowitą sumę iloczynów wag i interakcji równą 4.1.

Szanse/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga

O1	0	0	0	0.4	0	0	2
O2	0	0	1	0.4	1	0,4	1
O3	0	0	0	0.2	0	0	2
Waga	0.4	0.3	0.3				
Liczba interakcji	0	0	1				
Iloczyn wag i interakcji	0	0	0,3				
Ranga	2	2	1				

Tabela 4.56 Identyfikacja interakcji szans i słabych stron dla metody Smart Lock - opracowanie własne

W tabeli 2.56 widoczne są interakcje odpowiadające na pytanie „Czy szanse pozwolą na przezwyciężenie słabych stron metody?”. Ich łączna liczba wyniosła 1, co daje 11% maksymalnej sumy. Suma wszystkich iloczynów wag i interakcji wyniosła 0.7.

Zagrożenia/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	1	1	1	0.3	3	0,9	2
T2	1	1	1	0.6	3	1,8	1
T3	0	1	1	0.1	2	0,2	3
Waga	0.4	0.3	0.3				
Liczba interakcji	2	3	3				
Iloczyn wag i interakcji	0,8	0,9	0,9				
Ranga	2	1	1				

Tabela 4.57 Identyfikacja interakcji zagrożeń i słabych stron dla metody Smart Lock - opracowanie własne

Tabela 2.57 obrazuje odpowiedzi na pytanie „Czy ewentualne zagrożenia wzmocnią słabe strony?”, gdzie łączna suma interakcji wyniosła 8, dając 88% maksymalnego wyniku. Suma iloczynów wag i interakcji wyniosła 5.5.

Kombinacja	Wynik analizy SWOT	
	Suma interakcji	Suma iloczynów
S/O	4	2.6
S/T	0	0
W/O	4	2.4
W/T	7	4.8

Tabela 4.58 Zestawienie zbiorcze wyników analizy SWOT dla metody Smart Lock

Kombinacja	Wynik analizy TOWS	
	Suma interakcji	Suma iloczynów
O/S	7	4.8
T/S	6	4.1
O/W	1	0.7
T/W	8	5.5

Tabela 4.59 Zestawienie zbiorcze wyników analizy TOWS dla metody Smart Lock

Na podstawie zbiorczych zestawień wyników analizy interakcji z tabel 2.58 oraz 2.59 można ustalić strategię dla metody autoryzacji twarzą, co przedstawione zostało w tabeli 2.60.

Mocne strony [S]	**Szanse [O]**	**Zagrożenia [T]**
	Maxi-maxi	Maxi-mini
Suma interakcji	11	6
Suma iloczynów	7.4	4.1
Słabe strony [W]	Mini-maxi	Mini-mini
Suma interakcji	5	15
Suma iloczynów	3.1	10.3

Tabela 4.60 Wybór strategii na podstawie wyników analizy dla metody Smart Lock

W tabeli 2.60 najwyższą liczbę interakcji oraz iloczynów dla omawianej metody otrzymała strategia mini-mini. Oznacza to że jest ona narażona na wiele niekorzystnych czynników zewnętrznych i przeważają u niej słabe strony. Głównym zidentyfikowanym problemem jest mnogość sytuacji w których Smart Lock jest możliwy do obejścia, czy to

celowo czy nawet przez niedoskonałości metody lub błędy użytkownika. Należy dodać że Smart Lock na urządzeniach z systemem Android nie może być wykorzystany jako jedyna metoda odblokowania urządzenia – najczęściej jest alternatywą do odblokowania wzorem lub kodem PIN, ale nie jest to rozwiązanie zapewniające poziom zabezpieczeń wspomnianych metod, ponieważ można je obejść właśnie poprzez wykorzystanie luk Smart Locka. Nie jest to więc metoda zapewniająca odpowiedni poziom bezpieczeństwa użytkownika, z tego też powodu nie jest tak powszechnie wykorzystywana, zazwyczaj jedynie w pojazdach po połączeniu z systemem audio poprzez Bluetooth aby ułatwić kierowcy szybkie skorzystanie z urządzenia. Niezaprzeczalnym atutem tej metody jest wygoda przez nią oferowana, co wpłynęło na wysoki wynik w kierunku strategii maxi-maxi. Można powiedzieć, że metoda ta jest praktycznie bezobsługowa, gdyż po skonfigurowaniu odpowiednich warunków urządzenie będzie zawsze odblokowane dla użytkownika. Niestety ten wysoki poziom ułatwień został okupiony znacznym obniżeniem poziomu bezpieczeństwa.

4.6. Odcisk palca kluczem do urządzenia

Kod	Czynniki wewnętrzne		Kod	Czynniki zewnętrzne	
	Waga	Mocne strony		Waga	Szanse
S1	0.4	Wygoda, brak konieczności pamiętania czegokolwiek	O1	0.5	Różne możliwości implementacji czytników – w przycisku, w obudowie czy pod ekranem
S2	0.2	Metoda korzysta z cechy unikalności linii papilarnych co utrudnia podrobienie odcisku palca	O2	0.3	Aktywny rozwój czytników zwiększający ich precyzję i szybkość
S3	0.4	Szybkość – autoryzacja zajmuje mniej czasu niż np. wpisanie PIN'u lub skan twarzy	O3	0.2	Możliwość weryfikacji tożsamości w zewnętrznych serwisach na podstawie odcisku palca
Kod	**Waga**	**Słabe strony**	**Kod**	**Waga**	**Zagrożenia**
W1	0.6	Narażenie prywatności użytkownika poprzez przechowywanie jego danych biometrycznych	T1	0.6	Czytniki mogą mieć problemy z odczytaniem zabrudzonych lub wilgotnych palców
W2	0.1	Możliwość odblokowania urządzenia po podrobieniu lub zdobyciu odcisku palca	T2	0.2	Osoby trzecie mogą uzyskać dostęp do urządzenia przez manipulację użytkownika, np. użycie odcisku palca osoby śpiącej lub nieświadomej
W3	0.3	Dobrej jakości czytniki linii papilarnych	T3	0.2	Możliwość nadużycia lub wykradnięcia danych biometrycznych użytkownika

		zwiększają koszt urządzeń			

Tabela 4.61 Oszacowanie siły wpływu poszczególnych czynników na dobór strategii autoryzacji odciskiem palca - opracowanie własne

Mocne strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	1	0	0	0.4	1	0,4	2
S2	0	1	1	0.2	2	0,4	2
S3	1	1	0	0.4	2	0,8	1
Waga	0.5	0.3	0.2				
Liczba interakcji	2	2	1				
Iloczyn wag i interakcji	1	0,6	0,2				
Ranga	1	2	3				

Tabela 4.62 Identyfikacja interakcji mocnych stron i szans dla autoryzacji odciskiem palca – opracowanie własne

Tabela 2.62 przedstawia odpowiedzi na pytanie „Czy mocne strony metody pozwolą na wykorzystanie możliwych szans?”, które uzyskały sumę interakcji wynoszącą 5, dającą 55% maksymalnej liczby interakcji, a suma iloczynów wag i interakcji wyniosła 3.4.

Mocne strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.4	0	0	1
S2	0	0	0	0.2	0	0	1
S3	0	0	0	0.4	0	0	1
Waga	0.6	0.2	0.2				
Liczba interakcji	0	0	0				
Iloczyn wag i interakcji	0	0	0				
Ranga	1	1	1				

Tabela 4.63 Identyfikacja interakcji mocnych stron i zagrożeń dla autoryzacji odciskiem palca - opracowanie własne

W tabeli 2.63 zobrazowano analizę interakcji będących odpowiedziami na pytanie „Czy mocne strony metody pomogą w pokonaniu zagrożeń?”. Suma wszystkich interakcji wyniosła 0, jak również suma iloczynów.

Słabe strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	0	0.6	0	0	2
W2	0	0	1	0.1	1	0,1	1
W3	0	0	0	0.3	0	0	2
Waga	0.5	0.3	0.2				
Liczba interakcji	0	0	1				
Iloczyn wag i interakcji	0	0	0,2				
Ranga	2	2	1				

Tabela 4.64 Identyfikacja interakcji słabych stron i szans dla autoryzacji odciskiem palca - opracowanie własne

Tabela 2.64 ukazuje odpowiedzi na pytanie „Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans?”. Suma interakcji w tym przypadku wynosi 1, co daje 11% maksymalnej sumy tego układu. Suma iloczynów i wag interakcji równa jest 0.3.

Słabe strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	0	0	1	0.6	1	0,6	1
W2	0	1	0	0.1	1	0,1	2
W3	0	0	0	0.3	0	0	3
Waga	0.6	0.2	0.2				
Liczba interakcji	0	1	1				

Iloczyn wag i interakcji	0	0,2	0,2
Ranga	2	1	1

Tabela 4.65 Identyfikacja interakcji słabych stron i zagrożeń dla autoryzacji odciskiem palca - opracowanie własne

Interakcje stanowiące odpowiedzi na pytanie „Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń?" widoczne w tabeli 2.65 osiągnęły łączną liczbę wszystkich interakcji dającą 2, co stanowi 22% maksymalnej sumy interakcji. Suma iloczynów wag i interakcji osiągnęła wynik 1.1.

Szanse/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	1	0	1	0.5	2	1	1
O2	0	1	0	0.3	1	0,3	2
O3	0	1	0	0.2	1	0,2	3
Waga	0.4	0.2	0.4				
Liczba interakcji	1	2	1				
Iloczyn wag i interakcji	0,4	0,4	0,4				
Ranga	1	1	1				

Tabela 4.66 Identyfikacja interakcji szans i mocnych stron dla autoryzacji odciskiem palca - opracowanie własne

Tabela 2.66 ukazuje odpowiedzi na pytanie „Czy dostępne szanse zintensyfikują mocne strony metody?". Suma interakcji wyniosła tutaj 4, co daje 44% maksymalnego wyniku. Suma iloczynów wag i interakcji równa jest natomiast 2.7.

Zagrożenia/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga

T1	1	0	1	0.6	2	1,2	1
T2	0	1	0	0.2	1	0,2	2
T3	0	0	0	0.2	0	0	3
Waga	0.4	0.2	0.4				
Liczba interakcji	1	1	1				
Iloczyn wag i interakcji	0,4	0,2	0,4				
Ranga	1	2	1				

Tabela 4.67 Identyfikacja interakcji zagrożeń i mocnych stron dla autoryzacji odciskiem palca - opracowanie własne

Widoczne w tabeli 2.67 interakcje odpowiadające na pytanie „Czy odkryte zagrożenia osłabią mocne strony?" dają sumę równą 3, stanowiącą 33% maksymalnego wyniku, oraz całkowitą sumę iloczynów wag i interakcji wynoszącą 2.4.

Szanse/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	0	0	0	0.5	0	0	2
O2	0	1	0	0.3	1	0,3	1
O3	0	0	0	0.2	0	0	2
Waga	0.6	0.1	0.3				
Liczba interakcji	0	1	0				
Iloczyn wag i interakcji	0	0,1	0				
Ranga	2	1	2				

Tabela 4.68 Identyfikacja interakcji szans i słabych stron dla autoryzacji odciskiem palca - opracowanie własne

W tabeli 2.68 przedstawione są interakcje odpowiadające na pytanie „Czy szanse pozwolą na przezwyciężenie słabych stron metody?". Ich łączna liczba wyniosła 1, będąc 11% maksymalnej sumy. Suma iloczynów wag i interakcji wyniosła 0.4.

Zagrożenia/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	0	0	1	0.6	1	0,6	1
T2	0	1	0	0.2	1	0,2	2
T3	1	0	0	0.2	1	0,2	2
Waga	0.6	0.1	0.3				
Liczba interakcji	1	1	1				
Iloczyn wag i interakcji	0,6	0,1	0,3				
Ranga	1	3	2				

Tabela 4.69 Identyfikacja interakcji zagrożeń i słabych stron dla autoryzacji odciskiem palca - opracowanie własne

Tabela 2.69 zawiera odpowiedzi na pytanie „Czy ewentualne zagrożenia wzmocnią słabe strony?”. Łączna suma interakcji wyniosła 3 co stanowi 33% maksymalnego wyniku. Suma iloczynów wag i interakcji wyniosła 2.

Kombinacja	Wynik analizy SWOT	
	Suma interakcji	Suma iloczynów
S/O	5	3.4
S/T	0	0
W/O	1	0.3
W/T	2	1.1

Tabela 4.70 Zestawienie zbiorcze wyników analizy SWOT dla autoryzacji odciskiem palca

Kombinacja	Wynik analizy TOWS	
	Suma interakcji	Suma iloczynów
O/S	4	2.7
T/S	3	2.4
O/W	1	0.4
T/W	3	2

Tabela 4.71 Zestawienie zbiorcze wyników analizy TOWS dla autoryzacji odciskiem palca

Na podstawie zbiorczych zestawień wyników analizy interakcji z tabel 2.70 oraz 2.71 można określić strategię dla metody autoryzacji odciskiem palca, co przedstawione zostało w tabeli 2.72.

Mocne strony [S]	**Szanse [O]**	**Zagrożenia [T]**
	Maxi-maxi	Maxi-mini
Suma interakcji	9	3
Suma iloczynów	6.1	2.4
Słabe strony [W]	Mini-maxi	Mini-mini
Suma interakcji	2	5
Suma iloczynów	0.7	3.1

Tabela 4.72 Wybór strategii na podstawie wyników analizy dla autoryzacji odciskiem palca

W tabeli 2.72 największą sumę iloczynów dla metody autoryzacji odciskiem palca otrzymała strategia maxi-maxi. Świadczy to o przeważającej liczbie szans i mocnych stron metody. Taka strategia może sugerować, że powinno się przyłożyć dużą uwagę do rozwoju tej metody zarówno pod kątem technologicznym jak i możliwościami zastosowania. Oczywiście autoryzacja z wykorzystaniem linii papilarnych nie jest doskonała i posiada luki w zabezpieczeniach, które można wykorzystać, jednakże spośród omawianych do tej pory metod można stwierdzić że jest na to narażona w najmniejszym stopniu – głównie ze względu na trudność w podrobieniu odcisku palca tak, by został zaakceptowany przez skaner. Dodatkowo, ciągły rozwój technologii czytników odcisków utrudnia próby ich fałszerstwa za sprawą coraz to bardziej precyzyjnych i wymagających sensorów. Za tym rozwojem idzie również zwiększony koszt implementacji, ale jest to rozwiązanie na tyle powszechne, że wielu producentów posiada spore zasoby wiedzy i doświadczenia, które może być wspólnie wykorzystywane do ulepszania obecnych technologii związanych z tą metodą. Jednym z najbardziej istotnych faktów na który warto zwrócić uwagę jest największa popularność tej metody wśród użytkowników – obecnie zdecydowana większość urządzeń wypuszczanych na rynek jest wyposażona w czytnik odcisków palców w takiej lub innej formie. Czynnikami najbardziej wpływającymi na ten sukces są przede wszystkim szybkość i wygoda

oferowane przez tą metodę, które nie są uzyskiwane kosztem poziomu bezpieczeństwa danych użytkownika.

4.7. Uwierzytelnianie wieloskładnikowe (Multi Factor Authentication)

Kod	Czynniki wewnętrzne		Kod	Czynniki zewnętrzne	
	Waga	Mocne strony		Waga	Szanse
S1	0.3	Wymagane co najmniej dwa czynniki znacząco podnoszą poziom bezpieczeństwa	O1	0.5	Rosnąca popularność - MFA staje się standardem zabezpieczeń w wielu branżach
S2	0.1	Możliwość różnego łączenia czynników – PIN, SMS, klucz U2F i inne	O2	0.1	Możliwość wykorzystania posiadanego urządzenia jako dodatkowego czynnika (SMS lub aplikacja uwierzytelniająca)
S3	0.6	Wysoka odporność na ataki – atakujący muszą zdobyć wszystkie używane czynniki	O3	0.4	Polityki wymagające określonych typów czynników uznawanych za bardziej bezpieczne
Kod	**Waga**	**Słabe strony**	**Kod**	**Waga**	**Zagrożenia**
W1	0.5	Konieczność posiadania dostępu do wielu czynników przy każdej autoryzacji może być postrzegane jako niewygodne	T1	0.2	Zależność niektórych czynników od zasięgu czy dostępu do Internetu (kody SMS, aplikacje uwierzytelniające)
W2	0.3	Użytkownik może dobrać czynniki, które będą łatwe w zdobyciu, np. wykradnięcie hasła oraz kodu SMS z	T2	0.6	Mniej obeznani z technologią użytkownicy mogą zniechęcić się do MFA i uznać tą metodę za zbyt skomplikowaną jeśli

		wykorzystaniem ataków socjotechnicznych			nie zostaną odpowiednio wyedukowani
W3	0.2	Fizyczne składniki MFA jak klucze U2F lub dodatkowe urządzenia mogą być dużym kosztem dla użytkownika czy przedsiębiorstwa	T3	0.2	Rozwój nowych technik ataków przez cyberprzestępców mających na celu obejście MFA

Tabela 4.73 Oszacowanie siły wpływu poszczególnych czynników na dobór strategii autoryzacji MFA - opracowanie własne

Mocne strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	1	1	0	0.3	2	0,6	1
S2	0	1	1	0.1	2	0,2	2
S3	1	0	0	0.6	1	0,6	1
Waga	0.5	0.1	0.4				
Liczba interakcji	2	2	1				
Iloczyn wag i interakcji	1	0,2	0,4				
Ranga	1	3	2				

Tabela 4.74 Identyfikacja interakcji mocnych stron i szans dla autoryzacji MFA – opracowanie własne

W tabeli 2.74 ukazane zostały odpowiedzi na pytanie „Czy mocne strony metody pozwolą na wykorzystanie możliwych szans?”. Uzyskały one sumę interakcji wynoszącą 5, będącą 55% maksymalnej liczby interakcji. Suma iloczynów wag i interakcji wyniosła 3.

Mocne strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
S1	0	0	0	0.3	0	0	3
S2	1	0	0	0.1	1	0,1	2
S3	0	0	1	0.6	1	0,6	1
Waga	0.2	0.6	0.2				
Liczba interakcji	1	0	1				
Iloczyn wag i interakcji	0,2	0	0,2				
Ranga	1	2	1				

Tabela 4.75 Identyfikacja interakcji mocnych stron i zagrożeń dla autoryzacji MFA - opracowanie własne

W tabeli 2.75 przedstawiono analizę interakcji stanowiących odpowiedzi na pytanie „Czy mocne strony metody pomogą w pokonaniu zagrożeń?”. Suma wszystkich interakcji wyniosła 2, dając 22% maksymalnej sumy. Całkowita suma iloczynów wyniosła 1.1.

Słabe strony/Szanse	O1	O2	O3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	1	0	1	0.5	2	1	1
W2	0	1	0	0.3	1	0,3	3
W3	1	0	1	0.2	2	0,4	2
Waga	0.5	0.1	0.4				
Liczba interakcji	2	1	2				
Iloczyn wag i interakcji	1	0,1	0,8				
Ranga	1	3	2				

Tabela 4.76 Identyfikacja interakcji słabych stron i szans dla autoryzacji MFA - opracowanie własne

Tabela 2.76 obrazuje odpowiedzi na pytanie „Czy odkryte słabe strony metody będą przeszkodą w wykorzystaniu możliwych szans?”. Suma interakcji w tabeli wynosi 5, co stanowi 55% maksymalnej możliwej sumy. Suma iloczynów i wag interakcji osiągnęła wynik 3.9.

Słabe strony/Zagrożenia	T1	T2	T3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
W1	1	1	0	0.5	2	1	1
W2	0	0	1	0.3	1	0,3	2
W3	0	0	0	0.2	0	0	3
Waga	0.2	0.6	0.2				
Liczba interakcji	1	1	1				
Iloczyn wag i interakcji	0,2	0,6	0,2				
Ranga	2	1	2				

Tabela 4.77 Identyfikacja interakcji słabych stron i zagrożeń dla autoryzacji MFA - opracowanie własne

Interakcje odpowiadające na pytanie „Czy słabe strony metody zwiększą oddziaływanie na nią zagrożeń?” przedstawione w tabeli 2.77 uzyskały łączną liczbę wszystkich interakcji dającą 3, co stanowi 33% maksymalnej sumy interakcji. Suma iloczynów wag i interakcji równa jest 2.3.

Szanse/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
O1	1	0	1	0.5	2	1	1
O2	0	1	0	0.1	1	0,1	3
O3	0	0	1	0.4	1	0,4	2
Waga	0.3	0.1	0.6				

Liczba interakcji	1	1	2
Iloczyn wag i interakcji	0,3	0,1	1,2
Ranga	2	3	1

Tabela 4.78 Identyfikacja interakcji szans i mocnych stron dla autoryzacji MFA - opracowanie własne

Tabela 2.78 obrazuje odpowiedzi na pytanie „Czy dostępne szanse zintensyfikują mocne strony metody?”. Suma interakcji wyniosła w tym przypadku 4, co daje 44% maksymalnego wyniku. Suma iloczynów wag i interakcji natomiast równa jest 3.1.

Zagrożenia/Mocne strony	S1	S2	S3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	1	0	0	0.2	1	0,2	2
T2	1	1	0	0.6	2	1,2	1
T3	0	0	1	0.2	1	0,2	2
Waga	0.3	0.1	0.6				
Liczba interakcji	2	1	1				
Iloczyn wag i interakcji	0,6	0,1	0,6				
Ranga	1	2	1				

Tabela 4.79 Identyfikacja interakcji zagrożeń i mocnych stron dla autoryzacji MFA - opracowanie własne

Przedstawione w tabeli 2.79 interakcje odpowiadające na pytanie „Czy odkryte zagrożenia osłabią mocne strony?” dają całkowitą sumę równą 4, będącą 44% maksymalnego możliwego wyniku, oraz sumę iloczynów wag i interakcji dającą 2.9.

Szanse/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga

O1	0	0	1	0.5	1	0,5	1
O2	0	0	1	0.1	1	0,1	3
O3	0	1	0	0.4	1	0,4	2
Waga	0.5	0.3	0.2				
Liczba interakcji	0	1	2				
Iloczyn wag i interakcji	0	0,3	0,4				
Ranga	3	2	1				

Tabela 4.80 Identyfikacja interakcji szans i słabych stron dla autoryzacji MFA - opracowanie własne

W tabeli 2.80 zobrazowane są interakcje odpowiadające na pytanie „Czy szanse pozwolą na przezwyciężenie słabych stron metody?”. Całkowita liczba interakcji wyniosła 3, dając 33% maksymalnej sumy. Suma iloczynów wag i interakcji osiągnęła wynik 1.7.

Zagrożenia/Słabe strony	W1	W2	W3	Waga	Liczba interakcji	Iloczyn wag i interakcji	Ranga
T1	1	0	0	0.2	1	0,2	2
T2	1	1	0	0.6	2	1,2	1
T3	0	1	0	0.2	1	0,2	2
Waga	0.5	0.3	0.2				
Liczba interakcji	2	2	0				
Iloczyn wag i interakcji	1	0,6	0				
Ranga	1	2	3				

Tabela 4.81 Identyfikacja interakcji zagrożeń i słabych stron dla autoryzacji MFA - opracowanie własne

Tabela 2.81 przedstawia odpowiedzi na pytanie „Czy ewentualne zagrożenia wzmocnią słabe strony?”, gdzie łączna suma interakcji wyniosła 4 co stanowi 44% maksymalnego wyniku. Suma iloczynów wag i interakcji wyniosła natomiast 3.2.

Kombinacja	Wynik analizy SWOT	
	Suma interakcji	Suma iloczynów
S/O	5	3
S/T	2	1.1
W/O	5	3.9
W/T	3	2.3

Tabela 4.82 Zestawienie zbiorcze wyników analizy SWOT dla autoryzacji MFA

Kombinacja	Wynik analizy TOWS	
	Suma interakcji	Suma iloczynów
O/S	4	3.1
T/S	4	2.9
O/W	3	1.7
T/W	4	3.2

Tabela 4.83 Zestawienie zbiorcze wyników analizy TOWS dla autoryzacji MFA

Na podstawie zbiorczych zestawień wyników analizy interakcji z tabel 2.82 oraz 2.83 można ustalić strategię dla metody autoryzacji z wykorzystaniem MFA, co przedstawione zostało w tabeli 2.84.

Mocne strony [S]	**Szanse [O]**	**Zagrożenia [T]**
	Maxi-maxi	Maxi-mini
Suma interakcji	9	6
Suma iloczynów	6.1	4
Słabe strony [W]	Mini-maxi	Mini-mini
Suma interakcji	8	7
Suma iloczynów	5.6	5.5

Tabela 4.84 Wybór strategii na podstawie wyników analizy dla autoryzacji MFA

Jak można zauważyć w tabeli 2.84 największą sumę interakcji oraz iloczynów otrzymała strategia maxi-maxi, jednakże zbliżone, wysokie wyniki uzyskały także mniej optymistyczne strategie jak mini-maxi i mini-mini. Najważniejszym czynnikiem

stojącym za tym faktem jest to, że użytkownicy bardzo często przedkładają wygodę ponad bezpieczeństwo. Autoryzacja z wykorzystaniem wielu czynników nie należy do grona tych metod, które poświęcają bezpieczeństwo na rzecz ułatwień dla korzystającego – wręcz przeciwnie, tutaj wygoda została świadomie ograniczona na rzecz bardzo wysokiego poziomu zabezpieczeń. Właśnie to podejście przeważyło finalnie o wyborze strategii maxi-maxi, ponieważ dzięki swojej charakterystyce metoda ta znajduje na rynku coraz więcej zastosowań i jest coraz powszechniej i chętniej stosowana zarówno w miejscach pracy jak i przez osoby prywatne. Warto zwrócić uwagę, że jeżeli chodzi o dostępne czynniki MFA, to najwyższym poziomem bezpieczeństwa cechują się fizyczne klucze U2F, których obecność jest wymagana podczas autoryzacji. Oczywiście urządzenia te wiążą się z kosztami, ale firmy coraz bardziej skłonne są za nie zapłacić jeśli w grę wchodzi bezpieczeństwo danych ich klientów. Z tego też powodu powstały polityki wymuszające konkretny rodzaj czynników autoryzacji wieloskładnikowej, aby uniknąć sytuacji w której użytkownik skorzysta z dwóch czynników obarczonych dużym ryzykiem wykradnięcia lub złamania. W takim przypadku zalety MFA nie byłyby zauważalne, jeżeli osoby trzecie mogłyby z łatwością wejść w posiadanie składników autoryzacji. Można więc stwierdzić, że poziom bezpieczeństwa autoryzacji wieloskładnikowej uzależniony jest od poziomu bezpieczeństwa jej czynników.

5. Podsumowanie

Niniejsza praca miała na celu zbadanie istniejących metod autoryzacji w systemie Android oraz poddanie ich analizie zgodnie z wybraną metodą badawczą. Właściwe jest zatem podsumować w obecnym rozdziale wyniki badań autora. Dla każdej z analizowanych metod określona została strategia odpowiadająca jej charakterystyce ze względu na jej czynniki wewnętrzne jak i zewnętrzne. Przyporządkowanie strategii do poszczególnych metod zostało podsumowane w poniższej tabeli 3.1.

Nazwa metody autoryzacji	Strategia
Numeryczny kod PIN	Mini-mini
Alfanumeryczne hasło	Mini-mini
Blokada wzorem	Mini-maxi
Rozpoznawanie twarzy	Maxi-maxi
Smart-Lock	Mini-mini
Odcisk palca	Maxi-maxi
Multi Factor Authentication	Maxi-maxi

Tabela 5.85 Podsumowanie wybranych strategii dla metod autoryzacji

Metody autoryzacji, dla których określona została najbardziej niekorzystna strategia mini-mini nie oferowały same w sobie zadowalającego poziomu zabezpieczeń. Zarówno kod PIN jak i hasło bez odpowiednich polityk wymuszających na użytkowniku odpowiednią długość, złożoność i częstą zmianę, nie stanowią wyzwania dla cyberprzestępców z wydajnymi maszynami mogącymi złamać je w ciągu paru chwil, zwłaszcza jeśli użytkownicy używają prostych lub popularnych haseł. Tak więc bez zewnętrznych ograniczeń i wymagań mających na celu przypilnowanie użytkownika, metody te nie są wystarczająco bezpieczne.
Kolejną metodą z tą samą strategią jest Smart-Lock, który z uwagi na liczne możliwości obejścia przez osoby trzecie również nie osiągnął zadowalającego poziomu bezpieczeństwa. Twórcy tej metody przekazali dużą odpowiedzialność za prawidłowe funkcjonowanie na użytkownika, jednakże nie powinni oni w pełni mu ufać, gdyż nawet jeśli nie celowo to przypadkowo może on stworzyć sytuację w której pozostawi telefon bez nadzoru a ktoś uzyska do niego dostęp. Ciężko jest też dokładnie określić zasięg połączenia z zaufanym urządzeniem, zwłaszcza w pomieszczeniach z obiektami

blokującymi sygnały bezprzewodowe. Również dane dotyczące adresu zamieszkania nie stanowią w dzisiejszych czasach danych poufnych, co ułatwia określenie zaufanej lokalizacji. Te liczne sytuacje sprzyjające osobom niepożądanym sprawiły że metoda Smart-Lock nie uzyskała lepszego wyniku podczas analizy.

Następną strategią która pojawia się w zestawieniu jest mini-maxi. Określona została ona wyłącznie dla metody odblokowania wzorem. Jest ona bardzo popularna wśród użytkowników systemu Android, ale niestety nie umożliwia on modyfikacji rozmiaru siatki pól, a co za tym idzie złożoności wzoru. Taka opcja jest dostępna wyłącznie w zmodyfikowanych wersjach Androida, z których instalacją niekoniecznie poradzi sobie każdy użytkownik. Podobnie jak w przypadku kodu PIN i hasła, problemem jest tu także wykorzystywanie prostych wzorów, do odgadnięcia których nie potrzeba nawet zewnętrznego komputera. Ciekawym podejściem do tego problemu jest metoda odblokowania proponowana przez badaczy, polegająca na narysowaniu gestu na siatce pól składających się z losowych cyfr, wśród których znajdują się te właściwe, zdefiniowane przez użytkownika [16]. Jedyną trudność a zarazem dodatkowe zabezpieczenie dla metody odblokowania wzorem stanowi problem symulacji przeciągania palca po ekranie, z którym nie każdy cyberprzestępca łatwo sobie poradzi.

Strategia maxi-mini nie została określona dla żadnej z metod. Charakteryzuje się ona licznymi mocnymi stronami ale również i przewagą zagrożeń wokół danej metody. Analiza nie wykazała metody pasującej bezpośrednio do tych kryteriów.

Ostatnią strategią z opisywanych jest maxi-maxi, którą przyjęły trzy metody autoryzacji – rozpoznawanie twarzy, odcisk palca oraz MFA. Cechą wspólną dwóch pierwszych jest biometria. Jako metody korzystające z cech odróżniających ludzi, cieszą się największą popularnością wśród użytkowników, wykorzystując to co zawsze mają przy sobie – własne cechy biometryczne. Są to również czynniki bardzo trudne w podrobieniu, zwłaszcza biorąc pod uwagę wciąż rozwijane możliwości skanerów biometrycznych. Metody te oferują największą wygodę, nie obniżając tym samym poziomu bezpieczeństwa. Jedyne co jest objęte ryzykiem utraty to dane dotyczące właśnie twarzy czy odcisków palców użytkownika, jednakże zdecydowana ich większość godzi się z tym faktem na rzecz wspomnianej wcześniej wygody. Przechodząc do metody uwierzytelniania wieloskładnikowego, można stwierdzić że jest ona najbardziej efektywna w połączeniu z fizycznymi czynnikami jak klucze U2F lub kodami jednorazowymi z aplikacji uwierzytelniającej czy wiadomości SMS. Jest to cecha

wspólna z poprzednimi metodami o tej samej strategii – one wymagają fizycznej obecności użytkownika, natomiast MFA wymaga posiadania fizycznego czynnika określonego przez niego. Różnicą między nimi jest jednak poziom oferowanej wygody, która w autoryzacji wieloskładnikowej nie jest zbyt zadowalająca z perspektywy przeciętnego użytkownika. Również warunkiem utrzymania wysokiego poziomu zabezpieczeń jest to, że użytkownik nie skonfiguruje jako czynników metod o niskim poziomie bezpieczeństwa.

6. Wnioski

Można z całą pewnością stwierdzić, że najistotniejszym czynnikiem wpływającym na poziom bezpieczeństwa oferowany przez daną metodę autoryzacji jest sam użytkownik. Niezależnie czy metoda jest łatwa w złamaniu jak kod PIN, czy trudna w obejściu jak MFA, jeżeli użytkownik nie będzie uważny i zaniecha podstawowych środków ostrożności oraz nie będzie przestrzegać zaleceń dotyczących konfiguracji danej metody – zawsze znajdzie się jakaś powstała z tego powodu luka możliwa do wykorzystania przez osoby trzecie. Dlatego tak ważne jest, aby producenci w swoich urządzeniach implementowali polityki wymuszające na użytkowniku określone normy bezpieczeństwa, dla dobra jego danych i jego samego. Na ile jest to możliwe warto również korzystać z metod określonych jako bardziej bezpieczne, tj. tych opisanych strategią maxi-maxi. Oczywiście MFA niekoniecznie jest rozsądnym rozwiązaniem jeśli chodzi o odblokowywanie urządzenia, ale jako zabezpieczenie wrażliwych aplikacji lub ustawień – jak najbardziej.

Z uwagi na wciąż rozwijającą się technologię, możliwe jest powstanie z biegiem czasu kolejnych metod autoryzacji, lepszych lub gorszych od obecnie istniejących. Badacze przewidują, że polegać one będą w głównej mierze na zintegrowaniu ze sobą wielu czynników, korzystających z wiedzy użytkownika, biometrii lub faktu fizycznego posiadania klucza dostępu [17]. Metody istniejące już dzisiaj mogą także ewoluować i wpłynąć na oferowany poziom bezpieczeństwa. Niemniej jednak najistotniejszym wnioskiem jest fakt, że wraz z postępującym rozwojem metod autoryzacji, które mają na celu chronić dane użytkownika, równie szybko postępują metody ich kompromitacji, tworzone przez osoby czerpiące zyski z nielegalnego wykorzystania danych użytkowników. Bardzo ważna jest edukacja wśród społeczeństwa odnośnie istniejących zabezpieczeń, mająca na celu zwiększenie ich świadomości w tym temacie. Nie ważne jak wysoki będzie poziom zabezpieczeń oferowany przez metodę, jedynie użytkownik świadomie korzystający z dostępnych narzędzi ochrony danych, może wykorzystać ich pełen potencjał.

Autor niniejszej pracy stwierdza, że cel jakim była analiza metod autoryzacji w systemie Android pod kątem bezpieczeństwa, został zrealizowany. Dzięki określeniu strategii dla każdej z metod możliwe jest również wskazanie metod charakteryzujących

się zdecydowanie wysokim, a także stanowczo niskim poziomem zapewnianego bezpieczeństwa.

Z całą pewnością analiza mogłaby zostać poszerzona o większą ilość czynników mających wpływ na metody, a także o badania dotyczące tego, jak dużą wagę mają dla szerszego grona faktycznych użytkowników poszczególne czynniki. Analizę można również wzbogacić o porównanie złożoności pomiędzy danymi metodami, co również pomogłoby w uszeregowaniu ich względem odporności na ataki *brute force*.

Zdaniem autora należne byłoby w ramach rozwinięcia pracy przeprowadzenie testów na fizycznych urządzeniach, które polegałyby na próbach sforsowania zabezpieczeń poszczególnych metod, wykorzystując wiedzę dotyczącą słabych stron i zagrożeń wpływających na nie. Pozwoliłoby to zobrazować jak podatne mogą być zabezpieczenia i jak łatwo można je złamać posiadając odpowiednią wiedzę.

Podczas tworzenia niniejszej pracy autor poznał zarówno wady i zalety rozwiązań, które sam stosuje na co dzień. Proces analizy wymagał dogłębnego rozeznania danej metody i zidentyfikowania wpływających na nią czynników. Wiedza ta skłoniła autora do rozważenia rezygnacji z bardziej podatnych metod jak odblokowanie zaufanym urządzeniem w pobliżu poprzez Smart Lock, oraz do uświadomienia o potencjalnych zagrożeniach osób wokół niego, które korzystają z równie skrajnie niebezpiecznych metod. Samo uświadomienie jednak nie jest wystarczające, gdyż użytkownik uświadomiony o zagrożeniu, wciąż może się na nie świadomie godzić – kwestią decydującą jest jak bardzo ten użytkownik ceni sobie bezpieczeństwo swoich danych.

7. Wykaz literatury

[1] S. Szmitka, *Analiza SWOT jako narzędzie oceny innowacyjności przedsięwzięcia biznesowego,* Warmińsko-Mazurski Kwartalnik Naukowy, Nauki Społeczne nr 4, 2015, s. 80

[2] J. Sadłowska-Wrzesińska, R. Marczewska-Kuźma, A. Jakubowicz, *Możliwości zastosowania analizy SWOT/TOWS w procesie projektowania koncepcji bezpieczeństwa behawioralnego,* w *Zeszyty Naukowe Politechniki Poznańskiej,* 2020, nr 81 str. 186

[3] Fundacja Instytut Cyberbezpieczeństwa, *Autoryzacja*, źródło: https://instytutcyber.pl/encyklopedia/autoryzacja/ , dostęp 09.09.2024

[4] Fundacja Instytut Cyberbezpieczeństwa, *Autentykacja*, źródło: https://instytutcyber.pl/encyklopedia/autentykacja/ , dostęp 09.09.2024

[5] DataGenetics – PIN analysis, źródło: http://www.datagenetics.com/blog/september32012/ , dostęp 09.09.2024

[6] System operacyjny Android - https://www.android.com/intl/pl_pl/ , dostęp 09.09.2024

[7] *Complete list of PIN-blocks*, https://www.eftlab.com/knowledge-base/complete-list-of-pin-blocks , dostęp 09.09.2024

[8] *Android Management API – PasswordQuality, https://developers.google.com/android/management/reference/rest/v1/PasswordRequirements?hl=pl ,* dostęp 09.09.2024

[9] *Average unlocks per day among smartphone users in the United States as of August 2018, by generation*, https://www.statista.com/statistics/1050339/average-unlocks-per-day-us-smartphone-users/ , dostęp 09.09.2024

[10] P. Andriotis, G. Oikonomou, A. Mylonas, T. Tryfonas, *A Study on Usability and Security Features of the Android Pattern Lock Screen*, 2016, źródło: https://andriotisp.github.io/assets/pdf/ics16andrio.pdf , dostęp 09.09.2024

[11] Iris scanner - Samsung, źródło: https://www.samsung.com/hk_en/support/mobile-devices/galaxy-s8-iris-scanner/ , dostęp 09.09.2024

[12] 3D Face Recognition – Huawei, źródło: https://consumer.huawei.com/uk/support/faq/how-to-enable-face-recognition/ , dostęp 09.09.2024

[13] Project Soli, źródło: https://www.infineon.com/dgdl/Infineon-Google+Soli+FAQ+Document-FAQ-v03_00-EN.pdf?fileId=5546d4625d5945ed015d9845149e04c4 , dostęp 09.09.2024

[14] K. Kowalik, *Analiza SWOT-TOWS jako narzędzie wyboru strategii funkcjonowania-case study,* Archiwum Wiedzy Inżynierskiej Tom 5 nr 1, 2020, źródło: https://www.qpij.pl/attachment/id/863 , dostęp 09.09.2024

[15] J. Sadłowska-Wrzesińska, R. Marczewska-Kuźma, A. Jakubowicz, *Możliwości zastosowania analizy SWOT/TOWS w procesie projektowania koncepcji bezpieczeństwa behawioralnego,* Zeszyty Naukowe Politechniki Poznańskiej nr 81, 2020, źródło: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-5447a316-1234-4eb9-a040-44ddf249a058/c/sadlowska_joanna_mozliwosci_81_2020.pdf , dostęp 09.09.2024

[16] P. Król, D. Marek, J. Smołka, *Analysis of user behavior and authorization methods in context of mobile devices security,* Journal of Computer Sciences Institute 6, str. 34-41, 2018, źródło: https://www.researchgate.net/publication/337172460_Analysis_of_user_behavior_and_authorization_methods_in_context_of_mobile_devices_security , dostęp 09.09.2024

[17] C. Wang, Y. Wang, Y. Chen, H. Liu, J. Liu, *User authentication on mobile devices: Approaches, threats and trends,* 2020, s. 19, źródło: https://www.sciencedirect.com/science/article/am/pii/S1389128618312799 , dostęp 09.09.2024

8. Spis rysunków

9. Spis tabel