Nr 1(74) 2019

ISSN 2544-7068

BEZPIECZNY BANK

BFG
BANKOWY
FUNDUSZ
GWARANCYJNY

BEZPIECZNY BANK jest czasopismem wydawanym przez Bankowy Fundusz Gwarancyjny od 1997 roku, poświęconym zagadnieniom stabilności systemu finansowego, ze szczególnym uwzględnieniem systemu bankowego.

Artykuły publikowane w BEZPIECZNYM BANKU są recenzowane.
Za publikację naukową w BEZPIECZNYM BANKU Minister Nauki i Szkolnictwa Wyższego przyznał trzynaście punktów.
BEZPIECZNY BANK (online) ISSN 2544-7068
Wcześniejsze wydania BEZPIECZNEGO BANKU miały numer ISSN 1429-2939

REDAKCJA

Krystyna Kawerska

WYDAWCA

Bankowy Fundusz Gwarancyjny
ul. Ks. Ignacego Jana Skorupki 4
00-546 Warszawa

SEKRETARIAT REDAKCJI

Ewa Teleżyńska
Telefon: 22 583 08 78
e-mail: redakcja@bfg.pl

Informacje dotyczące wymogów formalnych i edytorskich dla autorów publikacji znajdują się na stronie: **www.bfg.pl**

DOM WYDAWNICZY ELIPSA

Opracowanie komputerowe:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel. 22 635 03 01, e-mail: elipsa@elipsa.pl,
www.elipsa.pl

Nr 1(74) 2019 Bezpieczny Bank

DOI: 10.26354/bb.7.1.74.2019

Miscellanea

Piotr Kałużny*
ORCID: 0000-0002-3153-9485
Piotr Stolarski**
ORCID: 0000-0001-7076-2316

Biometria behawioralna i „tradycyjna“ w mobilnych usługach bankowych – stan oraz przyszłe możliwości zastosowania

Streszczenie

W artykule scharakteryzowano tradycyjne (fizyczne) i behawioralne metody biometryczne, możliwe do wykorzystania w procesach uwierzytelniania w bankowości w urządzeniach mobilnych. Zaproponowano model uwierzytelniania za pomocą biometrii behawioralnej, który może zostać wdrożony w sektorze usług finansowych. Dokonano też analizy metod uwierzytelniania w bankowości, ze szczególnym uwzględnieniem metod zabezpieczeń wykorzystywanych w systemach informatycznych. Scharakteryzowano również stan rynku usług płatności mobilnych. Wreszcie wskazane zostały praktyczne implikacje zastosowania metod biometrycznych w usługach bankowych wraz z dyskusją przykładowych scenariuszy stosowania metod biometrii behawioralnej.

Słowa kluczowe: biometria, biometria behawioralna, uwierzytelnianie, bankowość, aplikacje mobilne, bankowość elektroniczna, bankowość mobilna

JEL: G21, G32, D9, D18

* Doktorant w Katedrze Informatyki Ekonomicznej na Wydziale Informatyki i Gospodarki Elektronicznej Uniwersytetu Ekonomicznego w Poznaniu.
** Doktor w Katedrze Informatyki Ekonomicznej na Wydziale Informatyki i Gospodarki Elektronicznej Uniwersytetu Ekonomicznego w Poznaniu.

Behavioral and traditional biometrics in mobile financial services – current state and future outlook

Abstract

The article characterizes traditional (physical) and behavioral biometrics methods, which can be applied in authentication procedures in banking on mobile devices. Moreover, the model of authentication with the use of behavioral biometric methods was presented. Such model may be used in the future banking applications. A wide overview of authentication methods in banking is presented in the article, including current state of the mobile payment market and a summary of the most important concepts and ideas connected with the authentication methods used in information systems. The text also presents practical implications resulting from the use of behavioral methods in the financial sector and the discussion over the example scenarios of proposed methods.

Key words: biometrics, behavioral biometrics, authentication, banking, mobile applications, e-banking, mobile banking

Wstęp

Aktualne zmiany w systemach bankowości – oraz płatności – są m.in. wynikiem intensywnego rozwoju technologii, w tym obserwowanego zwiększenia udziału usług mobilnych. Pojawianie się nowych systemów płatności, jak np. Blik, rodzi potrzebę opracowania dopasowanych do nich systemów zabezpieczeń. Badania ankietowe wskazują, że klienci banków przeważnie nie są w stanie ocenić, na ile bezpieczne są używane przez nich aplikacje mobilne[1]. Kwestia bezpieczeństwa i świadomości klientów jest tym bardziej istotna, że liczba użytkowników mobilnych aplikacji bankowych stale rośnie. W badaniach ankietowych przeprowadzonych w 2016 roku dla polskiego rynku wśród 1000 osób pracujących i studiujących w Łodzi odsetek osób korzystających z tego typu usług wyniósł 88% badanych. Podobny wynik – 85% respondentów w grupie wiekowej 18–34 lata – uzyskano w niedawnym badaniu[2] „Digital Payments 2017" firmy VISA przeprowadzonym dla całej Europy. Dodatkowo z badania tego płyną następujące wnioski: użytkownicy za najważniejszy czynnik w korzystaniu z aplikacji bankowych uważają wygodę, wolą nie nosić ze sobą gotówki, jednocześnie w niewiele mniejszym stopniu interesuje ich bezpieczeństwo oferowanych usług. Te oczekiwania użytkowników powodują, że nowe rozwiązania przygotowane dla banków i instytucji finansowych muszą uwzględniać pojawiające się technologie oraz trendy, dążąc do kompromisu między funkcjonalnością a bezpieczeństwem.

[1] M. Staszczyk, *Ochrona konsumentów korzystających z usług bankowości elektronicznej na przykładzie ankiety przeprowadzonej wśród osób pracujących i/lub studiujących w Łodzi*, „Bezpieczny Bank" 2016, 1 (62), s. 149–164; J. Imgraben, A. Engelbrecht i K.R. Choo, *Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users*, Behaviour & Information Technology 2014, 33.12, pp. 1347–1360.

[2] Visa. *Visa – Digital Payments Study 2017 ikonografika*. https://www.visa.pl/onas/aktualnosci/infografika-digital-payments-study-2017-71231.

Przykładem takiego trendu jest wykorzystanie biometrii. Metody biometryczne pozwalają na równoczesne zachowanie dużej wygody i bezpieczeństwa rozwiązania. Ich zastosowanie może jednak wywołać obawy dotyczące bezpieczeństwa samego wzorca biometrycznego oraz skuteczności działania takich metod w praktyce. Fakt pojawienia się i upowszechniania usług realizowanych na urządzeniach mobilnych uprawnia do postawienia pytania, czy dane generowane przez samo urządzenie nie mogą zostać wykorzystane do usprawnienia realizacji usług. Pozytywna odpowiedź zakłada wykorzystanie właśnie biometrii behawioralnej. Artykuł ma na celu porównanie biometrii behawioralnej z tradycyjnymi[3] metodami oraz zaprezentowanie możliwych scenariuszy jej wykorzystania w usługach bankowych.

1. Rynek płatności i aplikacji mobilnych

Z opracowania prezentującego wyniki badan VISA – „Digital Payments Study 2017" przeprowadzonych w Polsce[4] można dowiedzieć się, że 77% badanych używa smartfonów do zarządzania finansami osobistymi i codziennych płatności. 69% natomiast korzysta z portfela elektronicznego (np. PayPal), z usługi umożliwiającej zapisania danych karty w sklepie internetowym lub z form płatności mobilnych, tj. Android Pay. Konsumenci coraz chętniej dokonują transakcji na urządzeniach mobilnych[5]; obecnie połowa Polaków robi zakupy mobilnie (średnia europejska wynosi 48%). Zgodnie z badaniami Mastercard[6] udział klientów bankowości mobilnej w IV kwartale 2016 r. wyniósł 55% wszystkich klientów bankowości elektronicznej, co przekłada się na 18% klientów bankowości ogółem (patrz rysunek 1). Porównując powyższe dane z wynikami raportu PWC przygotowanego dla Niemiec w 2017 r.[7] , udział klientów bankowości mobilnej w roku 2017 dla tamtego rynku wynosi 13%, czyli zdecydowanie mniej niż w Polsce. Co ciekawe, grupa osób skłonnych do wykorzystania mobilnych metod płatniczych wskazana w badaniu PWC to aż 42% respondentów. Oznacza to możliwość osiągnięcia na rynku niemieckim dużego wzrostu tych usług w przyszłości.

[3] Autorzy utożsamiają „tradycyjne" metody biometryczne z biometrią fizyczną, która funkcjonowała wcześniej niż rozpatrywane w tekście metody behawioralne.

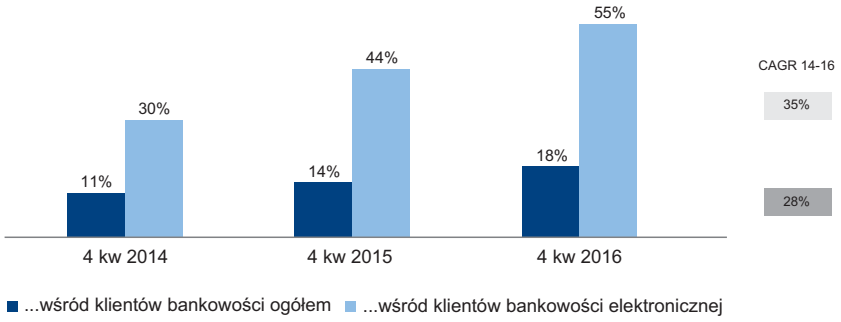
[4] *Visa – Digital Payments Study 2017*. https://www.visa.pl/o-nas/ aktualnosci/upowszechnienie-pieniadza-mobilnego-w-polsce-77percent-badanych-uzywa-smartfonow-do-bankowania-i-codziennychplatnosci-2190949.

[5] Za użytkownika płatności mobilnych uznano osobę, która korzysta z telefonu, tabletu czy urządzenia ubieralnego (wearable) do zarządzania swoimi pieniędzmi lub dokonywania płatności w sklepach stacjonarnych, Internecie lub poprzez aplikację.

[6] Mastercard. *Raport Mastercard Bankowość mobilna – trendy i wyróżniki oferty w Polsce i na świecie*. http://konferencje.alebank.pl/wp-content/uploads/2017/06/PM.Bankowosc-mobilna.Adam_.Splawski.Mastercard.pdf

[7] PwC. Mobile Payment Report 2017. https://www.pwc.de/mobilepayment

Rysunek 1. Klienci bankowości mobilnej na tle klientów bankowości ogółem (Mastercard)



Źródło: Mastercard. *Raport Mastercard Bankowość mobilna..., op. cit.*

Wracając do rodzimego rynku usług transakcyjnych, zgodnie z raportem VISA, głównym elementem wskazywanym jako przeszkoda w akceptacji i korzystaniu z nich jest bezpieczeństwo. Odsetek Polaków wyrażających obawy związane z poufnością wrażliwych danych wynosi obecnie aż 54%. Jednakże metody uwierzytelniania biometrycznego stają się coraz bardziej popularne, i to nie tylko wśród usługodawców. 83% konsumentów uważa je za bezpieczne (odsetek ten poparty jest też innymi badaniami[8]). Oznacza to, że zastosowanie i upowszechnianie metod biometrycznych, z zachowaniem odpowiedniej dbałości o bezpieczeństwo, może stać się w najbliższej przyszłości podstawą powstania przewagi konkurencyjnej poprzez budowanie wizerunku innowacyjności oraz wiarogodności. Konsumenci mogą preferować powierzenie procesu uwierzytelniania i przechowywania danych z nim związanych bankom jako instytucjom darzonym przez konsumentów zaufaniem. Powstawanie i rozwój nowych technologii powoduje rosnącą liczbę płatności w systemach mobilnych, do których muszą dostosować się systemy bezpieczeństwa. Przykładem może być zastosowanie technologii NFC (w zasadzie obecnie zastąpionej przez HCE – Host Card Emulation[9]). Technologia ta pozwala na wykorzystanie smartfonu w taki sam sposób jak tradycyjnej karty płatniczej. Z technologii HCE korzysta już wielu operatorów dostarczających systemy płatności, jak GooglePay, PeoPay czy od 2018 roku ApplePay.

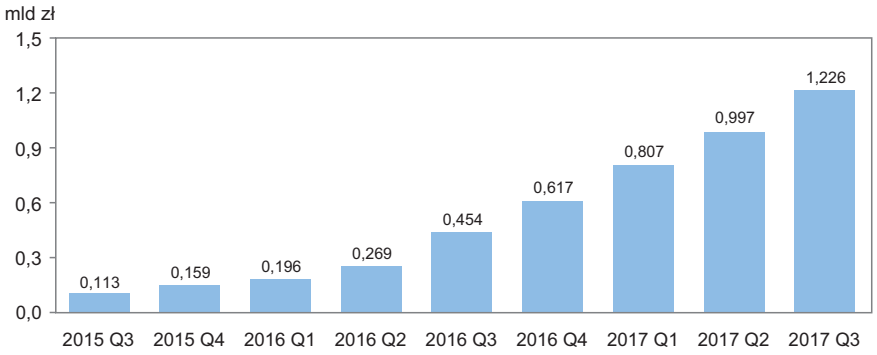
Drugim nieco odmiennym rozwiązaniem jest BLIK, pozwalający na wykorzystanie urządzeń przenośnych w celu dokonania płatności w zróżnicowanym środowisku biznesowym. Płatności realizowane są zarówno przy zakupach w Internecie, jak i w tradycyjnych sklepach, punktach usługowych, komunikacji miejskiej oraz urzędach publicznych. System BLIK jest w zasadzie kontynuatorem wcześniejszych rozwiązań, jak aplikacje iKasa czy IKO. Jednak w odróżnieniu od nich BLIK działa na dużo większą skalę i jest nowocześniejszy. Na koniec września 2017 r. system BLIK

[8] Związek Banków Polskich, *Biometria w bankowości i administracji publicznej*, Warszawa 2009.

[9] J. Uryniuk, *Alior, ING i SGB wycofują z oferty płatności mobilne NFC. Usługa będzie dostępna już tylko w dwóch bankach*. https://www.cashless.pl/wiadomosci/platnosci-mobilne/2174-alior-ing-i-sgb-wycofuja-z-ofertyplatnosci-mobilne-nfc-usluga-bedzie-dostepna-juz-tylko-w-dwochbankach

obejmował swoim zasięgiem 7 banków w Polsce z 5,3 mln użytkowników (liczba zarejestrowanych aplikacji mobilnych BLIK) oraz 75 192 sklepów internetowych[10] – dynamika systemu widoczna jest na rysunku 2.

Rysunek 2. Wartość zleceń zrealizowanych w systemie BLIK w kolejnych kwartałach (BLIK funkcjonuje od 09.02.2015 r.)



Źródło: Narodowy Bank Polski.

2. Metody uwierzytelniania i biometria

Proces uwierzytelniania i udzielania dostępu do dowolnego systemu (np. bankowości elektronicznej) wykorzystuje trzy podstawowe kategorie czynników[11]: *coś co wiemy* – hasła, numery PIN, odpowiedzi na sekretne pytania; *coś co posiadamy* – karty, dodatkowe urządzenia, tokeny; *to jacy jesteśmy* – wzorce biometryczne.

Metody biometryczne[12] polegają na dążeniu do określenia i zmierzenia pewnego zestawu cech obiektów, możliwych do zidentyfikowania i zapisu. Zapis cech unikalnych dla danego obiektu pozwala na jego identyfikację (ang. *identification*), natomiast dopasowanie zestawu cech obserwowanego obiektu do wcześniej zapamiętanego wzorca umożliwia uwierzytelnienie, czyli potwierdzenie tożsamości (ang. *authentication*). Działaniem uzupełniającym wymienione dwa poprzednie jest autoryzacja (ang. *authorization*) – upoważnienie, które polega na udzieleniu odpowiednich uprawnień na podstawie ich uprzedniego przypisania do obiektu.

[10] Narodowy Bank Polski (NBP). Informacja o rozliczeniach pieniężnych i rozrachunkach międzybankowych w III kwartale 2017 r. https://www.nbp.pl/systemplatniczy/publikacje/2017_3.pdf?v=20171023

[11] R.M. Bolle i in., *Guide to biometrics*, Springer Science & Business Media, 2013.

[12] W języku angielskim istnieje wyraźne rozróżnienie między *biometry* – gdy mówi się o pozyskiwaniu i analizie informacji o cechach w aspekcie biostatystyki i populacji, oraz *biometrics* – w przypadku zastosowań dotyczących identyfikacji i uwierzytelniania za ich pomocą – K. Saeed, *Biometrics principles and important concerns*, Biometrics and Kansei Engineering. Springer, 2012, s. 3–20.

Z metodami tymi związane jest pojęcie biometrii, które nie ma jednoznacznej definicji, a które zostało wnikliwie opisane w artykule Szymona Cegiełki[13]. Cechy mierzone w ramach biometrii charakteryzują się różnorodnymi własnościami, jak[14]:

- uniwersalność / powszechność (ang. *universality*) – cecha powinna być przypisana każdemu z badanych obiektów;
- unikalność lub rozróżnialność / indywidualność (ang. *uniqueness, distinctiveness*) – cecha powinna być wystarczająco różnorodna; nie musi być unikalna dla każdego obiektu, ale w praktyce powinna pozwolić na rozróżnienie obiektów (użytkowników)[15];
- łatwość akwizycji, ściągalność (ang. *ease of collecting / collectability*) – procesy pozyskania i zmierzenia cechy powinny być co najmniej możliwe, a najlepiej łatwe do przeprowadzenia;
- trwałość, niezmienność (ang. *persistence / permanence*) – cecha i jej skwantyfikowane wartości powinny pozostać niezmienne wraz z upływem czasu.

W literaturze wymienia się także inne własności pożądane ze względów praktycznych: parametry wydajnościowe systemu (ang. *efficiency, performance*) – rozumiane jako szybkość pobrania i dokładność klasyfikacji, odporność na próby fałszerstwa/niepodrabialność (ang. *circumvention, safety*) oraz akceptowalność (ang. *acceptability*). Nie każdej z cech biometrycznych będzie można przypisać wszystkie wymienione własności w stopniu maksymalnym[16].

Postępująca cyfryzacja usług wymusza na użytkownikach konieczność zapamiętywania bardzo wielu haseł, co może powodować frustrację[17] oraz zmniejszenie poziomu bezpieczeństwa ze względu na wykorzystywanie tego samego hasła dla różnych usług. Korzystanie z dodatkowych urządzeń generujących jednorazowe kody (tokeny) ogranicza się do zastosowań o wymaganym bardzo wysokim poziomie bezpieczeństwa, gdzie dodatkowe koszty i spadek użyteczności są uzasadnione ryzykiem złamania zabezpieczeń. Coraz częściej obserwuje się jednak sytuację odwrotną – smartfon staje się odpowiednikiem generatora kodów, przez który użytkownik uwierzytelnia się w innych usługach (płatności BLIK, NFC, 3-D Secure, logowanie oparte na OAuth). Wraz z dynamiką rozwoju usług mobilnych powoduje to rosnące wymagania co do poziomu bezpieczeństwa samych urządzeń przenośnych, aby zapewnić odpowiednią jakość usług i zapobiegać nadużyciom. Nie tylko producenci urządzeń, ale i usługodawcy dążą do dostosowania i zagwarantowania odpowiedniego poziomu bezpieczeństwa w swoich aplikacjach. Muszą także brać

[13] Sz. Cegiełko, *Kultura użytkowa zabezpieczeń biometrycznych klientów banków w Polsce na podstawie sondażu internetowego*, „Bezpieczny Bank" 2018, 3 (72), s. 164–184. DOI: 10.26354/bb.8.3.72.2018

[14] Związek Banków Polskich, *Biometria w bankowości...*, *op. cit.*; R.M. Bolle i in., *Guide to biometrics..*, *op. cit.*; A. Jain, L. Hong i S. Pankanti, *Biometric identification*, Communications of the ACM 2000, 43.2, s. 90–98.

[15] E.J. Kindt, *An Introduction into the Use of Biometric Technology*, [w:] *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013, s. 15–85.

[16] A. Jain, L. Hong i S. Pankanti, *Biometric identification...*, *op. cit.*, s. 90–98.

[17] Lawless Research, *Beyond the Password: The Future of Account Security*. https://www.telesign.com/wpcontent/uploads/2016/06/Telesign-Report-Beyondthe-Password-June-2016-1.pdf

pod uwagę złe nawyki użytkowników. Użytkownicy nie zawsze są skłonni do korzystania z systemów najbardziej bezpiecznych, poszukując raczej kompromisu pomiędzy bezpieczeństwem a użytecznością[18].

Jednym ze sposobów realizacji innowacyjnych usług wysokiej jakości na urządzeniach mobilnych, przy jednoczesnym zapewnieniu odpowiedniego poziomu bezpieczeństwa, jest wykorzystanie biometrii jako czynnika uwierzytelniania. Wykorzystanie metod biometrycznych nie powoduje po stronie użytkownika dodatkowej uciążliwości polegającej na obciążaniu pamięci (hasła) lub konieczności noszenia dodatkowych urządzeń. W porównaniu do tradycyjnych metod zabezpieczeń metody biometryczne pozwalają klientom na pewne, szybkie i wygodne[19] uwierzytelnianie w realizacji usług płatniczych i bankowych, zapewniając zarówno bezpieczeństwo, jak i wysoką użyteczność oferowanych usług. Zgodnie z badaniem Visa[20] dwie trzecie użytkowników chciałyby mieć dostęp do usług stosujących biometrię, która ich zdaniem jest dostatecznym czynnikiem zabezpieczającym.

3. Charakterystyka metod wykorzystujących cechy fizyczne i behawioralne

Cechy biometryczne można podzielić na fizyczne („tradycyjne") i behawioralne**,** podział ten pojawia się nawet w ugruntowanych i podstawowych pozycjach literaturowych[21]. Każda z cech może zostać zmierzona, a następnie przekształcona we wzorzec za pomocą metod różniących się precyzją i stopniem skomplikowania. Oprócz charakterystyk fizycznych, które wynikają bezpośrednio z zewnętrznie obserwowalnych cech biologicznych, można także mówić o cechach stanowiących przedmiot pomiaru biometrii behawioralnej – opisujących zróżnicowane wzorce zachowań, nie uwarunkowane biologicznie. Wzorce takie mogą być również wykorzystane jako cechy w systemie biometrycznym. Przykładowy podział, uwzględniający różnorodne aspekty i powszechnie używane cechy, został przedstawiony w tabeli 1. Należy zwrócić uwagę, że klasyfikacja ta nie ma charakteru wyczerpującego[22].

[18] C. Braz, J.M. Robert, *Security and usability: the case of the user authentication methods*, IHM 2006, Vol. 6, s. 199–203.

[19] Ł. Zakonnik i P. Czerwonka, *Płatności mobilne w Polsce – Analiza SWOT*, Studia i Materiały Polskiego Stowarzyszenia Zarządzania Wiedzą, 2014, 71.

[20] Visa. *European consumers ready to use biometrics for securing payments 2017*. https://www.visaeurope.com/newsroom/news/european-consumers-ready-forbiometrics.

[21] R.M. Bolle i in., *Guide to biometrics...*, *op. cit.*; K. Saeed, *Biometrics principles and important concerns*, Biometrics and Kansei Engineering. Springer 2012, s. 3–20; E.J. Kindt, *An Introduction into the Use of Biometric Technology*, [w:] *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013, s. 15–85.

[22] Nie obejmuje on także skomplikowanych w wykorzystaniu dla urządzenia mobilnego cech fizycznych, jak np. próbkowanie DNA, pomiar zapachu, termogram czy porównywanie kształtu ucha. Także metody behawioralne nieużyteczne z perspektywy urządzeń mobilnych, tj. profilowanie profilu ruchu myszy nie zostały uwzględnione.

Tabela 1. Podział cech biometrycznych

Rodzina cech	Cechy
Biometryki (cechy) fizyczne	twarz, siatkówka, tęczówka, odcisk palca, odcisk dłoni
Biometryki (cechy) behawioralne	gesty, dynamika pisania, profil dotyku (haptyka), chód, podpis, głos, profil behawioralny

Źródło: na podstawie A. Alzubaidi i J. Kalita, *Authentication of smartphone users using behavioral biometrics*, IEEE Communications Surveys & Tutorials 18.3 (2016).

Aby można było porównywać metody bądź wybierać odpowiednie do określonego zadania, trzeba zdefiniować kryteria pozwalające te metody jednoznacznie ocenić. Podstawowym celem uwierzytelniania jest dopasowanie faktycznych danych odpowiadających cechom użytkownika do tych zarejestrowanych wcześniej i zakodowanych w formie informacji lub wiedzy. Praktycznie niemożliwe jest uzyskanie wyników kolejnych pomiarów w 100% odpowiadających wzorcowi zapisanemu podczas rejestracji. Dlatego systemy uwierzytelniania operują na odpowiednich dla cechy metodach porównawczych, które dopuszczają określony margines odchyleń od wzorca. Wskazać można dwa typy błędów i związane z nimi metryki, które reprezentują względną jakość poszczególnych metod[23].

Pierwszy rodzaj błędu dotyczy sytuacji, gdy system nie przyznaje dostępu użytkownikowi, który faktycznie jest tym za kogo się podaje. Taki odsetek liczony w stosunku do wszystkich prób zalogowania się użytkownika nazywamy FRR (ang. *False Rejection Rate*). Drugi błąd to sytuacje, gdy nieuprawniony użytkownik (którego wzorzec jest podobny, lub który stara się imitować oryginalnego właściciela wzorca) uzyskuje dostęp do systemu – nazywany FAR (ang. *False Accept Rate*). Dla porównania różnych systemów zabezpieczania stosuje się także miarę EER (ang. *Equal Error Rate*) – oznaczającą poziom, dla którego wartości FAR i FRR są sobie równe. W przypadku systemów uwierzytelniania nie zawsze obie miary FAR oraz FRR są dla nas równie ważne. Na przykład przy próbie realizacji nieuprawnionego przelewu FRR możemy nie być pewni tożsamości użytkownika, natomiast FAR możemy zrozumieć jako udane przypadki oszustwa. Interpretacja pożądanego stosunku obu tych wartości zależy od wagi skutków obu tych błędów. Są one także wzajemnie zależne, zwiększenie FRR oznacza zmniejszenie FAR – i odwrotnie.

Biometria fizyczna obejmuje cechy biologiczne danego obiektu, m.in.: odcisk linii papilarnych palca, skan twarzy, skan tęczówki, bądź obraz naczyń krwionośnych palca (ang. *fingervein*). Do tradycyjnych metod biometrycznych stosowanych w urządzeniach mobilnych należą: analiza odcisku palca i rozpoznawanie twarzy.

Tabela 2 przedstawia charakterystykę tradycyjnych metod biometrycznych zgodnie z omówionymi powyżej metrykami błędów.

[23] A.K. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics: personal identification in networked society*, Vol. 479, Springer Science & Business Media, 2006.

Tabela 2. Dokładność tradycyjnych cech biometrycznych

Cecha	Dokładność	Łatwość fałszerstwa / podrobienia	Łatwość zastosowania w urządzeniach mobilnych
Tęczówka	FAR 0.001%, FRR 0.1%, dla smartfonów 1–2% EER.	Niska	Niska
Odcisk palca	FAR 1%, FRR 0.000002%.	Średnia	Średnia (wymaga sensora o odpowiedniej jakości)
Skan twarzy	FAR 6%, FRR 0.1%.	Wysoka (zdjęcie)	Wysoka

Źródło: opracowanie własne, parametry dokładności na podstawie badań ZBP.

Biometria behawioralna wykorzystuje cechy wynikające z zachowań, które można zdefiniować jako: „każdą możliwą do odczytania i kwantyfikacji reprezentacją zachowań użytkownika, dla której można wyróżnić identyfikowalne i unikalne (bądź co najmniej stabilne) wzorce, które pozwalają na odróżnienie użytkowników i przeprowadzenie procesu identyfikacji i uwierzytelniania”[24]. Metody behawioralne nie miały do niedawna zastosowania komercyjnego. W miarę upowszechniania użycia telefonów komórkowych do potwierdzania tożsamości w różnorodnych usługach i aplikacjach powstała potrzeba rozwoju biometrii w nowym kierunku. Obecność w codziennym życiu urządzeń, posiadających bogaty zestaw sensorów, otworzyła drogę do opracowania rozwiązań badających biometryki zachowania. Dokładność pomiarów dokonywanych z zastosowaniem cech behawioralnych rośnie w miarę powstawania nowych metod i jest w tej chwili podobna do wyników uzyskiwanych przez uwierzytelnianie za pomocą analizy obrazu twarzy. Do cech badanych przez metody biometrii behawioralnej możemy zaliczyć:

- profil dotyku (ang. *touch / touchscreen / touch profile*) – sposób interakcji użytkownika z ekranem dotykowym urządzenia[25]. Analizowane w tym przypadku są także akcje i obserwowane specyficzne cechy standardowych gestów (podwójne kliknięcia, przesuwanie ekranu tzw. swipe, itp.)[26];
- gesty (ang. *gestures*, często używa się po prostu *hand-waving*, co nie jest poprawne) – gesty służące do uwierzytelniania, zdefiniowane explicite w systemie[27],

[24] P. Kałużny, *Behavioural Profiling Authentication Based on Trajectory Based Anomaly Detection Model of User's Mobility*, International Conference on Business Information Systems, Springer, 2017, s. 242–254.

[25] C. Bo i in., *Silentsense: silent user identification via touch and movement behavioral biometrics*, Proceedings of the 19th annual international conference on Mobile computing & networking, ACM, 2013, s. 187–190.

[26] L. Li, X. Zhao i G. Xue, *Unobservable re-authentication for smartphones*, NDSS, 2013, s. 1–16; A. Buriro i in., *Itsme: Multi-modal and unobtrusive behavioural user authentication for smartphones*, International Conference on Passwords, Springer, 2015, s. 45–61.

[27] M. Piekarczyk i M.R. Ogiela, *On using palm and finger movements as a gesture based biometrics*, Intelligent Networking and Collaborative Systems (INCOS), 2015 International Conference on. IEEE. 2015,

np. machanie dłonią. Niekoniecznie muszą wymagać interakcji z ekranem dotykowym, mogą zostać zarejestrowane np. przez kamerę, czujnik IR, bądź akcelerometr[28];

- styl pisania (ang. *keystroke*) – cechę tę można też określić jako analizę tempa pisania, jego liczbowej reprezentacji, a także specyfiki wykorzystywania klawiszy, błędów językowych itp.[29];
- profilowanie behawioralne (ang. *behavioral profiling*) – „identyfikujące użytkowników na podstawie sposobu, w jaki wchodzą w interakcje z usługami urządzenia mobilnego"[30]. Jest to złożona grupa cech, którą ostatnio charakteryzuje duża dynamika powstawania nowych metod[31]. Opierają się one na różnorodnych aspektach zachowania użytkownika, np.: interakcje z usługami i aplikacjami oraz innymi urządzeniami (np. hotspotami WIFI), profil poruszania się (geograficzny);
- chód (ang. *gait*). W odróżnieniu od metod profilowania behawioralnego opiera się głównie na unikalności samego chodu, w oderwaniu od jego geograficznego aspektu. Zakres badań dotyczy też sposobu noszenia przez użytkownika urządzenia mobilnego (np. w kieszeni)[32];
- głos (ang. *voice*)[33]. Analiza głosu może dotyczyć zarówno aspektów technicznych samych fal dźwiękowych, jak i jej poziomu semantycznego i lingwistycznego[34]. W pewnych kontekstach[35] może być metodą, której użytkownik nie będzie chciał używać – np. podczas korzystania z usług transportu publicznego;

s. 211–216; J. Guerra-Casanova i in., *Authentication in mobile devices through hand gesture recognition*, International Journal of Information Security 2012 11.2, s. 65–83.

28 L. Yang i in., *Unlocking smart phone through handwaving biometrics*, IEEE Transactions on Mobile Computing 2015, 14.5, s. 1044–1055.

29 M. Karnan, M. Akila i N. Krishnaraj, *Biometric personal authentication using keystroke dynamics: A review*, Applied Soft Computing 2011, 11.2, s. 1565–1573; C. Giuffrida i in., *I sensed it was you: authenticating mobile users with sensor enhanced keystroke dynamics*, International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, 2014, s. 92–111; S.P. Banerjee i D.L. Woodard, *Biometric authentication and identification using keystroke dynamics: A survey*, „Journal of Pattern Recognition Research" 2012, 7.1, s. 116–139.

30 H. Saevanee i in., *Continuous user authentication using multi-modal biometrics*, Computers & Security 2015, 53, s. 234–246.

31 P. Kałuzny, *Behavioural Profiling...*, *op. cit.*, s. 242–254.

32 A. Primo i in., *Context-aware active authentication using smartphone accelerometer measurements*, Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on. IEEE. 2014, s. 98–105; T. Hoang i D. Choi, *Secure and privacy enhanced gait authentication on smart phone*, The Scientific World Journal 2014.

33 Głos ze względu na wysoki poziom skomplikowania przetwarzania, możliwą dużą zmienność oraz złożoność semantyczną odzwierciedlającą bogactwo języka naturalnego jest traktowany w tej pracy jako cecha behawioralna.

34 P. Tresadern i in., *Mobile biometrics (mobio): Joint face and voice verification for a mobile platform*, IEEE pervasive computing (2012); R.H. Woo, A. Park i T.J. Hazen, *The MIT mobile device speaker verification corpus: data collection and preliminary experiments*, Speaker and Language Recognition Workshop, 2006. IEEE Odyssey 2006: The. IEEE. 2006, s. 1–6.

35 A. Wójtowicz i K. Joachimiak, *Model for adaptable context-based biometric authentication for mobile devices*, Personal and Ubiquitous Computing 2016, 20.2, s. 195–207.

- podpis (ang. *signature*). Podobnie jak w przypadku głosu, aspekty grafologiczne oraz duża zmienność powodują, że tę cechę zaliczyć należy raczej do zbioru metod behawioralnych – w szczególności w przypadku systemów mobilnych[36].

Różnorodność możliwych do pomiaru cech oraz metody ich kwantyfikacji jest tematem wielu badań opisanych w aktualnej literaturze. Biometria behawioralna zakłada najczęściej jednoczesne użycie wielu cech będących przedmiotem pomiaru, co pozwala na zastosowanie wielu metod, w zależności od: kontekstu, sytuacji i stabilności wzorca pochodzącego od danego użytkownika. Dodatkowo wyróżnić można inne pożądane charakterystyki metod biometrycznych spełniane przez biometrię:

- Użyteczność i możliwość zastosowania w uwierzytelnianiu ciągłym (pasywnym) – Niektóre metody biometrii behawioralnej mogą działać pasywnie (ang. *continous authentication*), co pozwala na ciągłą aktualizację poziomu uwierzytelnienia, bez interakcji z użytkownikiem. Dzięki temu mogą być wykorzystywane do zwiększenia dokładności innych klasyfikatorów w procesie uwierzytelniania wieloczynnikowego (inaczej wieloskładnikowego lub multimodalnego (ang. *multi-factor authentication*)). Dodatkowo, ponieważ w wypadku uwierzytelniania pasywnego nie ma wymogu interakcji, nie skutkuje to utratą użyteczności przy wykorzystaniu wielu metod. Możliwe jest przez to jednoczesne zastosowanie wielu metod o dość wysokim stopniu błędów jako niezależnych klasyfikatorów, celem zmniejszenia końcowego poziomu błędu. W najnowszej literaturze przedstawiono bardzo interesujące badania dotyczące uwierzytelniania multimodalnego z wykorzystaniem twarzy, odcisku dłoni, głosu i podpisu[37]. Podobne badania byłyby wskazane do testowania rozwiązań uwierzytelniania ciągłego wraz z biometrią tradycyjną.
- Wykorzystanie niebinarnej miary porównań pozwala na ustalenie różnorodnych poziomów uwierzytelnienia i dostępu, w zależności np. od potencjalnych skutków oszustwa w przypadku nieuprawnionej próby użycia systemu. Można w ten sposób uzależnić operacje o wysokim ryzyku (np. przelew na znaczną kwotę) od większego poziomu zaufania w stosunku do porównanego wzorca. Natomiast operacje, które nie wymagają wysokiego poziomu pewności co do tożsamości użytkownika (np. sprawdzenie salda konta), mogą być autoryzowane przy średnim poziomie pewności. Dzięki zwiększonej użyteczności można obniżać częstość przeprowadzania procedury uwierzytelnienia.
- Możliwość podszycia się pod użytkownika – warto wskazać, że w zależności od charakterystyki cechy i metody wykorzystanej do ekstrakcji wzorca, możliwa jest próba jego skopiowania w celu podszycia się pod użytkownika. W przypadku odcisków palca możliwe jest oszukanie urządzenia za pomocą silikonowego

[36] G. Bailador i in., *Analysis of pattern recognition techniques for in-air signature biometrics*, Pattern Recognition 44.10-11 (2011), s. 2468–2478; M. Martinez-Diaz i in., *Mobile signature verification: Feature robustness and performance comparison*, IET Biometrics 2014, 3.4, s. 267–277.

[37] A. Czyżewski, P. Hoffmann, P. Szczuko, A. Kurowski, M. Lech & M. Szczodrak, *Analysis of results of large-scale multimodal biometric identity verification experiment*, IET Biometrics 2018, 8(1), s. 92–100.

odlewu[38] (wzorzec można uzyskać poprzez zdjęcie wysokiej rozdzielczości) lub wykonanie ataku słownikowego w celu odgadnięcia wzorca[39]. Do otrzymania wzorca twarzy może wystarczyć zdjęcie lub nagranie wideo z twarzą innego użytkownika[40]. Najnowsze technologie w celu przeciwdziałania takim atakom stosują skany w podczerwieni i dynamikę ruchu twarzy, choć wykonanie silikonowej maski pozwoliło na uzyskanie dostępu nawet do urządzenia zabezpieczonego takimi technologiami[41]. W przypadku głosu może wystarczyć nawet nagranie głosu wybranej osoby.

Niektóre metody pozwalają na łatwe uzyskanie kopii posiadanego wzorca, co w przypadku jego niezbywalności i trwałości może narazić użytkownika na znaczne szkody, a także wskazuje na zagrożenia płynące z uzyskania wzorca. Wyciek wzorca można przyrównać do wycieku hasła: może on nastąpić z wnętrza organizacji, która przechowuje wzorzec, ale również może mieć miejsce na zewnątrz organizacji. W tym drugim przypadku źródłem upublicznienia wzorca będzie inna organizacja lub usługa, w której użytkownik wykorzystuje ten sam wzorzec. W ten sposób uzyskanie wzorca ze słabiej zabezpieczonego systemu może stworzyć poważne zagrożenie dla użytkownika. Tym samym jedna z podstawowych charakterystyk, jaką jest trwałość cechy biometrycznej, może być przeszkodą w jej bezpiecznym stosowaniu. Warto zauważyć, że istnieją metody pozwalające na zwiększenie bezpieczeństwa wzorca dla metod biometrycznych wprowadzające „odwoływalne" wzorce (ang. *cancellable biometrics*[42]), które wykorzystują techniki łączenia wartości funkcji skrótu (ang. *hash*) i dodawania losowych elementów zależnych od dostawcy usługi do bazy sygnatur przechowywanej przez niego w trakcie procesu przesyłania lub przechowywania wzorca. Zmniejszają one skutki wycieku wzorca z repozytorium utrzymywanego przez dostawcę usługi. Dla zapewnienia pełnego bezpieczeństwa użytkownika muszą być jednak stosowane przez każdy podmiot realizujący usługi, co jest mało prawdopodobne, jeżeli uwzględnimy fakt, że liczba takich podmiotów przechowujących dane biometryczne wzrasta. Metody biometrii behawioralnej – przez charakterystykę zmienności wzorca w czasie oraz zależności od warunków i wykorzystanych metod, np. specyfiki urządzenia w przypadku profilu dotyku – pozwalają na zmniejszenie obawy o bezpieczeństwo wzorca. Dodatkowo, poprzez jednoczesne połączenie wielu metod i czynników, wzorzec biometrii behawioralnej jest trudny do odtworzenia i podrobienia. Systemy dobierające

[38] Hosseini Seyedehzahra, *Fingerprint vulnerability: A survey*. 2018 4th International Conference on Web Research (ICWR). IEEE, 2018.

[39] Roy Aditi i in., *Evolutionary methods for generating synthetic masterprint templates: Dictionary attack in fingerprint recognition*, 2018 International Conference on Biometrics (ICB). IEEE, 2018.

[40] J. Hernandez-Ortega, J. Fierrez, A. Morales, J Galbally, *Introduction to Face Presentation Attack Detection*, [w:] *Handbook of Biometric Anti-Spoofing*, Springer, 2019, Cham, s. 187–206.

[41] Bkav. http://www.bkav.com/d/top-news/-/view_content/content/103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions

[42] N. Radha i S. Karthikeyan, *An evaluation of fingerprint security using noninvertible biohash*, International Journal of Network Security & Its Applications (IJNSA) 2011, 3.4; V.M. Patel, N.K. Ratha i R. Chellappa, *Cancelable Biometrics: A review*, IEEE Signal Processing Magazine 2015, 32.5, s. 54–65. ISSN: 1053-5888. DOI: 10.1109/MSP.2015.2434151.

odpowiednie kombinacje cech (np. w zależności od kontekstu[43]) mają przewagę nad jednoskładnikowymi sposobami uwierzytelniania, zapewniając większe bezpieczeństwo wzorca.

Charakterystykę poprawy dokładności w rozróżnianiu użytkowników dla poszczególnych metod biometrii behawioralnej zawiera tabela 3. Mimo że pojedyncze aspekty wydają się charakteryzować niższą dokładnością, pojawiły się prace, które łącząc wiele z nich osiągały w uwierzytelnianiu ciągłym dla profilowania behawioralnego po 3 minutach 1% EER, albo w kombinacji dynamiki pisania z dodatkowymi sensorami były w stanie dla predefiniowanej frazy (hasła) osiągnąć 0,08% EER[44]. Najnowsze badania wskazują, że korzystając z wielu cech, można osiągnąć 99,98% dokładności uwierzytelniania przy poziomie błędu FAR równym 0,1%[45], co wskazuje na bardzo dynamiczne tempo rozwoju tych metod. Nie ustalono jeszcze wzorców w zakresie wykorzystanych transformacji danych i metryk porównań, ale są one w stanie konkurować z tradycyjnymi metodami biometrycznymi.

Tabela 3. Podział cech biometrii behawioralnej wraz z ich charakterystyką i wykorzystanymi metodami

Cecha	Dokładność	Czas potrzebny do uwierzytelnienia	Łatwość fałszerstwa	Łatwość użycia w urządzeniach mobilnych
Gesty	2% EER około 4% w przypadku odkrycia gestu[a]	1–2 s	Niska	Średnia
Podpis	0.29% EER[b], 2% EER[8] (4% w przypadku próby podrobienia znanego podpisu)[c].	Kilka sekund	Średnia	Niska
Głos	~2% EER (FAR 3%, FRR 0.1%)[d], potwierdzone dla urządzeń mobilnych[e].	1–2 s	Średnia	Wysoka
Nie wymagające dodatkowych interakcji				
Dynamika pisania	EER do około 1%[f]–2%[g,h]	Natychmiastowo, uwierzytelnianie ciągłe	Niska	Wysoka

[43] A. Wójtowicz i K. Joachimiak, *Model for adaptable context-based biometric authentication for mobile devices*, Personal and Ubiquitous Computing 2016, 20.2, s. 195–207.

[44] C. Giuffrida i in., *I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics...*, *op. cit.*, s. 92–111.

[45] D. Deb i in., *Actions Speak Louder Than (Pass) words: Passive Authentication of Smartphone Users via Deep Temporal Features*, arXiv preprint arXiv:1901.05107 (2019).

Cecha	Dokładność	Czas potrzebny do uwierzytelnienia	Łatwość fałszerstwa	Łatwość użycia w urządzeniach mobilnych
Profil dotyku	2–4 % EER[i]. Najlepsze wyniki wskazują 0.9 EER[j].	Natychmiastowo, uwierzytelnianie ciągłe	Niska	Wysoka
Chód	5,6% EER[k]. Inne źródła wskazują 3.92% FAR i FRR 11.76%[l].	Natychmiastowo, uwierzytelnianie ciągłe	Niska	Wysoka
Profilowanie behawio-ralne	EER 5% po 1 min i 1% po 3 min.[m] Inne źródła pokazują 2% EER[n]. Profilowanie behawio-ralne lingwistyczne wraz z dynamiką pisania 3.3% EER[o]	Natychmiastowo, uwierzytelnianie ciągłe	Bardzo niska	Wysoka

[a] J. Guerra-Casanova i in., *Authentication in mobile devices through hand gesture recognition*, „International Journal of Information Security" 2012, 11.2, s. 65–83.

[b] L. Yang i in., *Unlocking smart phone through handwaving biometrics*, IEEE Transactions on Mobile Computing 2015, 14.5, s. 1044–1055.

[c] M. Martinez-Diaz i in., *Mobile signature verification: Feature robustness and performance comparison*, IET Biometrics 2014, 3.4, s. 267–277.

[d] D. Thakkar, *Top Five Biometrics: Face, Fingerprint, Iris Palm, and Voice*, ed. by bayometric.com. https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

[e] L. Zou, Q. He i X. Feng, *Cell phone verification from speech recordings using sparse representation*, Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on. IEEE. 2015, s. 1787–1791.

[f] I. Lamiche i in., *A continuous smartphone authentication method based on gait patterns and keystroke dynamics*, „Journal of Ambient Intelligence and Humanized Computing" 2018, s. 1–14.

[g] V.M. Patel i in., *Continuous user authentication on mobile devices: Recent progress and remaining challenges*, IEEE Signal Processing Magazine 2016, 33.4, s. 49–61.

[h] S. Alotaibi, S. Furnell i N. Clarke, *Transparent authentication systems for mobile device security: A review*, Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for. IEEE. 2015, s. 406–413.

[i] W. Meng i in., *Surveying the development of biometric user authentication on mobile phones*, IEEE Communications Surveys & Tutorials 2015, 17.3, s. 1268–1293.

[j] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, A. Morales, *Benchmarking Touchscreen Biometrics for Mobile Authentication*, IEEE Transactions on Information Forensics and Security 2018, 13(11), 2720–2733. doi:10.1109/tifs.2018.2833042

[k] R. Damaševicius i in., *Smartphone user identity verification using gait characteristics*, Symmetry 2016, 8.10, s. 100.

[l] T. Hoang i D. Choi, *Secure and privacy enhanced gait authentication on smart phone*, The Scientific World Journal 2014.

[m] L. Fridman i in., *Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location*, IEEE Systems Journal 2017, 11.2, s. 513–521.

[n] F. Li i in., *Behaviour profiling for transparent authentication for mobile devices*, European Conference on Cyber Warfare and Security. Academic Conferences International Limited 2011, s. 307.

[o] H. Saevanee i in., *Continuous user authentication using multi-modal biometrics*, Computers & Security 2015, 53, s. 234–246.

Źródło: opracowanie własne na podstawie podanych źródeł.

4. Zastosowanie metod biometrycznych w praktyce

Rozpatrując zagadnienie wykorzystania biometrii w mobilnych rozwiązaniach dla sektora finansów, należy uwzględnić przynajmniej dwa aspekty. Z jednej strony smartfony stały się popularnym sprzętem znacznie ułatwiającym klientom dostęp do usług finansowych. Z drugiej zaś strony należy mieć świadomość, że ponad 40%[46] tego typu urządzeń pozostaje niezabezpieczonych (z powodu nieostrożności użytkowników) jakimkolwiek systemem zapobiegającym niepowołanemu dostępowi, co naraża ich na nieuprawniony dostęp do całości danych przechowywanych na urządzeniu. Użytkownicy równie często korzystają z takich samych haseł do różnych usług, a w skrajnych przypadkach zapisują te hasła na samym urządzeniu lub na kartce papieru; bywają także podatni na wiele innych możliwych technik ataku.

W 2016 roku niezależni eksperci razem z firmą Telesign[47] przygotowali raport podsumowujący odpowiedzi uzyskane w ankiecie przeprowadzonej wśród pracowników około 600 średnich i dużych przedsiębiorstw. Treść raportu przedstawia między innymi informacje o podstawowych źródłach niezadowolenia użytkowników związanych z procesem uwierzytelniania w systemach informatycznych. Najistotniejszymi z nich są: zapominanie haseł, odpowiadanie na sekretne pytania oraz konieczność wpisywania kodu PIN. Na podstawie raportu można stwierdzić, że uwierzytelnianie za pomocą metod biometrii jest uznawane przez użytkowników za najmniej kłopotliwe. Raport stwierdza jednocześnie, że badane firmy często korzystają z wielu różnych wieloczynnikowych systemów uwierzytelniania Odbywa się to zwykle kosztem użyteczności, bądź zastosowania bardziej skomplikowanych metod, co podnosi czasochłonność operacji. Dodatkowo ciężar uwierzytelnienia transakcji i wykrycia przypadków oszustwa (w rozumieniu ang. *fraud*) bywa przerzucany czy wręcz jest dobrowolnie przejmowany przez usługodawcę. Poza klasycznymi systemami antyfraudowymi (odchylenia od przeciętnych parametrów transakcji) uwierzytelnianie to odbywać się w interakcji z aplikacją – przez wykorzystanie wzorca behawioralnego, wzbogacającego dotychczasowe systemy antyfraudowe.

Do najczęściej wykorzystywanych metod biometrycznych w aplikacjach mobilnych należą: odcisk palca (ang. *fingerprint*) – odciski palca zaczęły być powszechnie stosowane dzięki technologii TouchID, którą wprowadzono na rynek w 2013 r., zaimplementowaną w urządzeniach z systemem IOs; skan twarzy (ang. *facial recognition*) – spopularyzowany przez Apple Face ID w 2018 r., gdy wprowadzono technologię skanowania w podczerwieni, skutecznie zwiększając jakość klasyfikatora (podobne rozwiązania zaczynają stosować także inni producenci sprzętu).

Wskazane powyżej technologie będą bez wątpienia dalej rozwijane i udoskonalane. Odcisk palca może być dość łatwo przekształcony poprzez wykorzystanie biometrii

[46] L. Fridman i in., *Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location*, IEEE Systems Journal 2017, 11.2, s. 513–521.

[47] Lawless Research. Beyond the Password: The Future of Account Security. https://www.telesign.com/wp-content/uploads/2016/06/Telesign-Report-Beyondthe-Password-June-2016-1.pdf (dostęp: 10.09.2016).

naczyń krwionośnych palca (ang. *Finger Vein*[48]), natomiast skan twarzy w dzisiejszych czasach jest wzbogacany przez trójwymiarowy model jej geometrii czy skan wykonany w podczerwieni. Należy również wspomnieć o innych metodach – jak skanowanie tęczówki – które są dostępne w niektórych urządzeniach mobilnych (np. Samsung Galaxy S8). W badaniach przeprowadzonych w roku 2017 odsetek światowych urządzeń z zainstalowanym czytnikiem linii papilarnych wahał się od 50% do 60%[49]. Jednak realny odsetek użycia tego sposobu uwierzytelniania może być taki sam jak dla tradycyjnych metod, a więc jedna trzecia urządzeń może nie posiadać aktywnego systemu uwierzytelniania.

Adaptacja wzorców biometrycznych w usługach sektora bankowego jest dość znacząca w porównaniu z innymi sektorami gospodarki wykorzystującymi rozwiązania informatyczne. Z opracowania przygotowanego przez serwis bankier.pl[50] wynika, że co najmniej 12 banków w Polsce (w tym wszystkie czołowe na rynku) pozwala na logowanie się do aplikacji za pomocą odcisku palca. Dwa banki pozwalają także na użycie innych metod biometrycznych (skan twarzy lub analiza próbki głosu) w celu dokonania uwierzytelnienia do bankowości mobilnej. Dodatkowo PKO BP prowadził testy tzw. bio-stanowisk umożliwiających weryfikację tożsamości z wykorzystaniem takich cech, jak: podpis, skan naczyń krwionośnych dłoni, głos czy skan twarzy. Ze względu na coraz powszechniejsze instalowanie w urządzeniach mobilnych różnego rodzaju czujników, zwiększy się udział aplikacji mobilnych wykorzystujących metody biometryczne. Należy spodziewać się, że w tym kierunku będzie też podążał rynek aplikacji związanych z sektorem finansowym, w tym z bankowością. Warto jednak podkreślić, że nawet szerokie upowszechnienie metod opartych na biometrii fizycznej nie wyeliminuje uciążliwości związanych z samym faktem konieczności poddania się procedurze uwierzytelnienia. Co najwyżej procedura ta będzie przebiegała mniej problematycznie w porównaniu do klasycznych sposobów zabezpieczeń systemów informatycznych. Wynika to z tego, że tradycyjna biometria oraz obecnie wykorzystywane metody mają dwie podstawowe cechy wspólne: binarny rezultat przeprowadzanego procesu kontroli użytkownika (uwierzytelnienie powiodło się lub nie) oraz konieczność umiejscowienia uwierzytelnienia jako osobnego kroku w całym procesie realizacji usługi przez użytkownika (metody wymagają od użytkownika interakcji polegającej na potwierdzeniu tożsamości).

[48] A. Urban i T. Woszczynski, *Biometryczne uwierzytelnianie klienta w oddziale bankowym*, „Gazeta Bankowa" 2012, 4, s. 86–87.

[49] TrendForce. Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018. https://press.trendforce.com/press/20180111-3049.html; DigiTimes. Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018. 2018. http://www.digitimes.com/news/a20160818PD208.html; androidauthority.com. Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018. https://www.androidauthority.com/2018-smartphones-fingerprint-sensors-803905/; statista.com. Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018. https://www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration/

[50] B. Wojciech, *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?*, 2017. https://www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html

Druga cecha oznacza, że każda operacja jest autoryzowana oddzielnie. Pod tym względem metody biometrii behawioralnej różnią się od tradycyjnej dość zasadniczo. Tutaj bowiem uwierzytelnianie może być procesem ciągłym odbywającym się niejako równolegle „w tle" (uwierzytelnianie pasywne). Autoryzacja może zatem być realizowana w sposób nie wymagający interakcji z użytkownikiem. Ponadto rezultat procesu identyfikacji użytkownika nie ma charakteru binarnego, lecz jest ciągłą miarą prawdopodobieństwa. Sytuacja taka ma oczywiście swoje zalety i wady. Zestawiając cechy biometrii behawioralnej z wcześniej wspomnianymi sposobami zabezpieczania systemów informatycznych, możemy stwierdzić, że metody te ze względu na wymienione różnice będą miały nieco odmienne zastosowania. W niektórych zaś przypadkach mogą się doskonale uzupełniać, tworząc środowiska o podwyższonym poziomie bezpieczeństwa, bez redukcji poziomu wygody użytkowania.

Fakt, że metody biometrii behawioralnej mogą nie dawać całkowitej pewności co do tożsamości użytkownika aplikacji, przynajmniej na razie uniemożliwia zastosowanie ich jako jedynego czynnika w procesie uwierzytelniania i autoryzacji. Z drugiej strony metodami tymi można dokonywać pomiarów w sposób ciągły, co pozwala na zastosowanie ich jako dodatkowego elementu zabezpieczeń czy wzbogacenie systemów antyfraudowych. W odróżnieniu od tradycyjnych zabezpieczeń, w biometrii behawioralnej, w zależności od sytuacji, można żądać różnego poziomu pewności określenia tożsamości podmiotu realizującego operację oraz oceny jego intencji. Rozpatrzmy dwa przykłady: sprawdzenie salda konta bankowego oraz transfer środków pieniężnych o znacznej wartości.

Pierwsza sytuacja mogłaby wymagać niższego poziomu pewności w zakresie autoryzacji niż druga, wymagająca zapewne wysokiego poziomu pewności. Ponieważ wiadomo jednak, że nawet tradycyjnie stosowane sposoby zabezpieczeń nie dają bezwzględnej gwarancji poprawności, więc nadal wskazania równolegle przeprowadzanych pomiarów biometrii behawioralnej mogą być zastosowane nadmiarowo w celu dodatkowego zmniejszenia ryzyka przeprowadzenia błędnej identyfikacji.

5. Scenariusze zastosowania biometrii behawioralnej w systemach płatniczych

Dla instytucji oferujących aplikacje mobilne realizujące transakcje finansowe jednym z najważniejszych aspektów jest maksymalizacja poziomu bezpieczeństwa. Jest to pojęcie wieloznaczne, na które może się składać wiele czynników. Jednak część z nich pozostaje pod kontrolą użytkownika (utrzymanie bezpieczeństwa hasła), zainteresowanego także wygodą oferowanych usług.

Jako potencjalne rozwiązanie powyższej sprzeczności celów można zaproponować zastosowanie biometrii behawioralnej w trzech podstawowych scenariuszach.

W pierwszym przypadku byłby to czynnik zwiększający użyteczność dzięki uwierzytelnianiu ciągłemu (pasywnemu). Dawałoby to możliwość zmniejszenia liczby

sytuacji wymagających weryfikacji tożsamości w sposób tradycyjny i pozwalałoby m.in. na zrealizowanie następującego scenariusza: użytkownik korzysta w aplikacji bankowej z mechanizmu zabezpieczenia przez odcisk palca, hasło albo PIN. Do uwierzytelniania normalnych transakcji, płatności NFC zwykle go nie potrzebuje. Występuje jednak anomalia – którą wykrywa działający w tle systemu biometrii behawioralnej, oznaczając akcję jako potencjalny przypadek fraudu. Dopiero wtedy wymagane jest potwierdzenie tożsamości innym czynnikiem uwierzytelniania.

W drugim przypadku wzrastałaby elastyczność usług – poprzez zastosowanie prawdopodobieństwa będącego wynikiem porównania obecnego zachowania z profilem biometrii behawioralnej użytkownika. Mechanizm taki może być połączony z określeniem innych procedur w zależności od obliczonego poziomu ryzyka akcji. Dzięki temu akcje o mniejszym ryzyku mogą wymagać mniejszej pewności uwierzytelnienia.

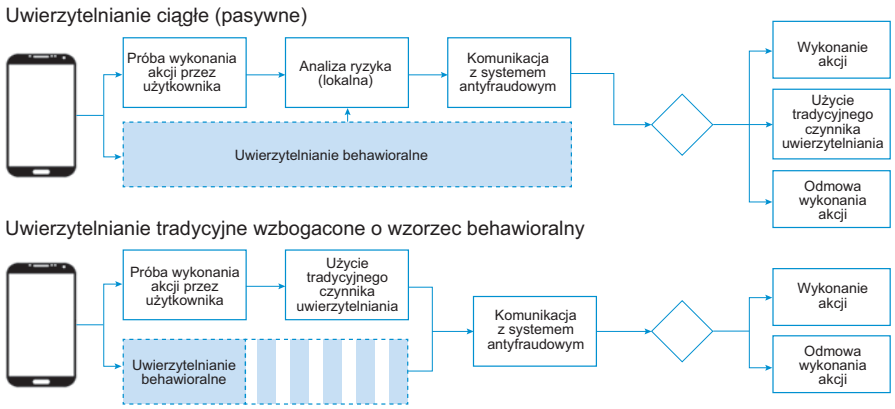
Wreszcie, w trzecim scenariuszu, byłby to czynnik poprawiający bezpieczeństwo – poprzez wzbogacenie tradycyjnego mechanizmu uwierzytelnienia profilem biometrii behawioralnej użytkownika, na przykład oprócz dotychczasowego czynnika (np. hasła) wykorzystując sygnaturę behawioralną (np. profil dotyku czy zachowania użytkownika) i uzyskując dodatkowe informacje.

Wykorzystane w biometrii behawioralnej algorytmy mogą się automatycznie uczyć na dostarczanych przez użytkowników danych. Każdy przypadek fraudu może pomóc globalnie w automatycznym wykrywaniu następnych. Dopasowanie algorytmów dla pojedynczych użytkowników, np. za każdym razem kiedy użytkownik zaloguje się poprawnie – mimo fałszywie wykrytego przez system fraudu – pozwoli zmniejszyć FRR (odsetek nieudanego uwierzytelnienia uprawnionego użytkownika). Algorytmy behawioralne pozwalają dodatkowo na rekomendację akcji poprzez połączenie «kontekstu» wykonywanej usługi z historią akcji użytkownika. Za pomocą badania profilu behawioralnego w aplikacji bankowej możemy np. zaproponować użytkownikowi autouzupełnienie formularza przelewu albo zlecenie stałe – jest to jednak dodatkowa funkcjonalność, z której użytkownik może zrezygnować.

W różnorodnych scenariuszach realizacji transakcji za pomocą kart lub urządzeń mobilnych wskazane byłoby wykorzystanie dodatkowych technik zabezpieczających. Warunkiem ich wprowadzenia musiałaby jednak być ich nieinwazyjność i transparentność z punktu widzenia użytkownika końcowego. Idealnym mechanizmem do zastosowania byłaby zatem jedna lub kilka połączonych metod biometrii behawioralnej. W przypadku zastosowania takich metod podstawowy schemat realizacji transakcji pozostałby niezmieniony. Natomiast jako oddzielny proces – lub wątki w trakcie korzystania z urządzenia mobilnego – dokonywane byłyby pomiary zachowań użytkownika. W momencie konieczności autoryzacji transakcji mechanizm działający w tle wskazywałby szacowane prawdopodobieństwo, że aplikacja jest w interakcji z prawowitym użytkownikiem, a więc podmiotem autoryzowanym do realizacji transakcji. Prawdopodobieństwo to, wynikające z oceny działającego systemu biometrii behawioralnej, umożliwiałoby określenie, czy urządzenie pozostaje pod kontrolą legalnego użytkownika. W szczególnym przypadku

wynik systemu, wyrażony prawdopodobieństwem, może być zaklasyfikowany jako jeden z trzech możliwych poziomów: wysoki – oznacza, że urządzenie jest pod kontrolą autoryzowanego użytkownika; średni – metody biometrii behawioralnej nie są w stanie jednoznacznie wskazać, jaki podmiot aktualnie używa urządzenia mobilnego; niski – prawdopodobnie urządzenie mobilne jest używane przez innego użytkownika. Realizacja scenariusza płatności mobilnej wraz z metodą zabezpieczeń biometrii behawioralnej zobrazowana została na diagramie przedstawionym na rysunku 3.

Rysunek 3. Scenariusze płatności mobilnej z wykorzystaniem metody zabezpieczeń biometrii behawioralnej



Źródło: opracowanie własne.

Podsumowanie

W pracy został scharakteryzowany rynek mobilnych aplikacji bankowych i finansowych oraz najnowsze trendy, mogące mieć w przyszłości zasadniczy wpływ na rozwój tego sektora. Jako jeden z kluczowych elementów została wskazana biometria, która pozwala na realizację usług mobilnych w sposób bezpieczny i wygodny, nie pozbawiony jednak pewnych ograniczeń. Zaprezentowano teoretyczne i praktyczne aspekty wykorzystania metod biometrycznych w mobilnych usługach płatniczych i bankowych do uwierzytelniania/autoryzacji użytkowników. Na podstawie analizy wskazano biometrię behawioralną jako jeden z kluczowych obszarów rozwoju tych metod. Scharakteryzowano ją na podstawie dostępnej literatury i badań oraz zaproponowano scenariusze wdrożenia metod w architekturze mobilnych usług. Poddano także dyskusji istotne cechy przemawiające za korzyściami płynącymi z wykorzystania metod biometrii behawioralnej, a także ich ograniczenia.

Bibliografia

Alotaibi S., Furnell S., & Clarke N., *Transparent authentication systems for mobile device security: A review*, Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for. IEEE, 2015.

Alzubaidi A., Kalita J., *Authentication of smartphone users using behavioral biometrics*, *IEEE Communications Surveys & Tutorials* 18.3 (2016).

Bailador G. i in., *Analysis of pattern recognition techniques for in-air signature biometrics*, [w:] *Pattern Recognition* 44.10-11 (2011).

Banerjee S.P., Woodard D.L., *Biometric authentication and identification using keystroke dynamics: A survey*, „Journal of Pattern Recognition Research" 2012, 7.1.

Blanco-Gonzalo R. i in., *Handwritten signature recognition in mobile scenarios: Performance evaluation*, 2012 IEEE International Carnahan Conference on Security Technology (ICCST), 2012.

Bo C. i in., *„Continuous user identification via touch and movement behavioral biometrics*, Performance Computing and Communications Conference (IPCCC), 2014 IEEE International. IEEE. 2014.

Bo C. i in., *Silentsense: silent user identification via touch and movement behavioral biometrics*, Proceedings of the 19th annual international conference on Mobile computing & networking. ACM. 2013.

Bolle R.M i in., *Guide to biometrics*, Springer Science & Business Media, 2013.

Buriro A. i in., *Itsme: Multi-modal and unobtrusive behavioural user authentication for smartphones*, International Conference on Passwords, Springer, 2015.

Braz C., Robert J.M., *Security and usability: the case of the user authentication methods*, IHM, 2006, Vol. 6.

Cegiełko Sz., *„Kultura użytkowa zabezpieczeń biometrycznych klientów banków w Polsce na podstawie sondażu internetowego*, „Bezpieczny Bank" 2018, 3 (72). DOI: 10.26354/bb.8.3.72.2018

Czyżewski A. i in., *Analysis of results of large-scale multimodal biometric identity verification experiment*, IET Biometrics 2018, 8(1).

Damaševicius R. i in., *„Smartphone user identity verification using gaitˇ characteristics*, Symmetry 2016, 8.10.

Deb D. i in., *Actions Speak Louder Than (Pass) words: Passive Authentication of Smartphone Users via Deep Temporal Features*, arXiv preprint arXiv:1901.05107 (2019).

Fridman L. i in., *Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location*, IEEE Systems Journal 2017, 11.2.

Giuffrida C. i in., *I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics*, International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2014.

Guerra-Casanova J. i in., *Authentication in mobile devices through hand gesture recognition*, „International Journal of Information Security" 2012, 11.2.

Hoang T., Choi D., *Secure and privacy enhanced gait authentication on smart phone*, The Scientific World Journal 2014.

Hosseini Seyedehzahra, *Fingerprint vulnerability: A survey*, 2018 4th International Conference on Web Research (ICWR). IEEE, 2018.

Imgraben J., Engelbrecht A., Choo K.R., *Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users*, Behaviour & Information Technology 2014, 33.12.

Jain A., Hong L., Pankanti S., *Biometric identification*, Communications of the ACM 2000, 43.2.

Jain A.K., Bolle R., Pankanti S., eds. *Biometrics: personal identification in networked society*, Vol. 479, Springer Science & Business Media, 2006.

Kałużny S., *Behavioural Profiling Authentication Based on Trajectory Based Anomaly Detection Model of User's Mobility*, International Conference on Business Information Systems, Springer, 2017.

Karnan M., Akila M., Krishnaraj N., *Biometric personal authentication using keystroke dynamics: A review*, Applied Soft Computing 2011, 11.2.

Kindt E.J., *An Introduction into the Use of Biometric Technology*, [w:] *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013.

Li F. i in., *Active authentication for mobile devices utilising behaviour profiling*, „International Journal of Information Security" 2014, 13.3.

Li F. i in., *Behaviour profiling for transparent authentication for mobile devices*, European Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2011.

Li L., Zhao X., Xue G., *Unobservable re-authentication for smartphones*, NDSS, 2013.

Martinez-Diaz M. i in., *Mobile signature verification: Feature robustness and performance comparison*, IET Biometrics 2014, 3.4.

Meng W. i in., *Surveying the development of biometric user authentication on mobile phones*, IEEE Communications Surveys & Tutorials 2015, 17.3.

Patel V.M., Ratha N.K., Chellappa R., *Cancelable Biometrics: A review*, IEEE Signal Processing Magazine 2015, 32.5. ISSN: 1053-5888. DOI: 10.1109/MSP.2015.2434151.

Patel V.M. i in., *Continuous user authentication on mobile devices: Recent progress and remaining challenges*, IEEE Signal Processing Magazine 2016, 33.4.

Piekarczyk M., Ogiela M.R., *On using palm and finger movements as a gesture-based biometrics*, Intelligent Networking and Collaborative Systems (INCOS), 2015 International Conference on, IEEE, 2015.

Primo A. i in., *Context-aware active authentication using smartphone accelerometer measurements*, Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on, IEEE, 2014.

Radha N., Karthikeyan S., *An evaluation of fingerprint security using noninvertible biohash*, „International Journal of Network Security & Its Applications (IJNSA)" 2011, 3.4.

Raja K.B. i in., *Multi-modal authentication system for smartphones using face, iris and periocular*, Biometrics (ICB), 2015 International Conference on, IEEE, 2015.

Roy Aditi i in., *Evolutionary methods for generating synthetic masterprint templates: Dictionary attack in fingerprint recognition*, 2018 International Conference on Biometrics (ICB), IEEE, 2018.

Saeed K., *Biometrics principles and important concerns*, Biometrics and Kansei Engineering, Springer, 2012.

Saevanee H. i in., *Continuous user authentication using multi-modal biometrics*, Computers & Security 2015, 53.

Staszczyk M., *Ochrona konsumentów korzystających z usług bankowosci elektronicznej na przykładzie ankiety przeprowadzonej wśród osób pracujących i/lub studiujących w Łodzi*, „Bezpieczny Bank" 2016, 1 (62).

Tresadern S. i in., *Mobile biometrics (mobio): Joint face and voice verification for a mobile platform*, IEEE pervasive computing, 2012.

Urban A., Woszczynski T., *Biometryczne uwierzytelnianie klienta w oddziale bankowym*, „Gazeta Bankowa" 2012, 4.

Wójtowicz A., Joachimiak K., *Model for adaptable context-based biometric authentication for mobile devices*, Personal and Ubiquitous Computing 2016, 20.2.

Woo R.H., Park A., Hazen T.J., *The MIT mobile device speaker verification corpus: data collection and preliminary experiments*, Speaker and Language Recognition Workshop, 2006, IEEE Odyssey 2006: IEEE, 2006.

Yang L. i in., *Unlocking smart phone through handwaving biometrics*, IEEE Transactions on Mobile Computing 14.5, 2015.

Zakonnik Ł., Czerwonka P., *Płatnosci mobilne w Polsce – analiza SWOT*, Studia i Materialy Polskiego Stowarzyszenia Zarzadzania Wiedzą/Studies & Proceedings Polish Association for Knowledge Management 71, 2014.

Zou L., Qianhua H., Xiaohui F., *Cell phone verification from speech recordings using sparse representation*, Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on, IEEE, 2015.

Związek Banków Polskich, *Biometria w bankowości i administracji publicznej*, Warszawa 2009.

Źródła internetowe

Androidauthority.com. *Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018*. https://www.androidauthority.com/2018-smartphones-fingerprint-sensors-803905/ (dostęp: 10.09.2018).

Boczoń W., Bankier.pl. *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?* https://www.bankier.pl/wiadomosc/Biometria-wbankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku7542743.html (dostęp: 10.09.2018).

Bkav „*Bkav's new mask beats Face ID in "twin way": Severity level raised, do not use Face ID in business transactions"* http://www.bkav.com/d/top-news//view_content/content/103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions (dostęp: 10.03.2019).

DigiTimes. *Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018*.

2018. http://www.digitimes.com/news/a20160818PD208.html (dostęp: 10.09.2018).

Mastercard. *Raport Mastercard Bankowość mobilna – trendy i wyróżniki oferty w Polsce i na świecie*, http://konferencje.alebank.pl/wp-content/uploads/2017/06/PM.Bankowosc-mobilna.Adam_.Splawski.Mastercard.pdf (dostęp: 10.09.2018).

Narodowy Bank Polski (NBP), Informacja o rozliczeniach pieniężnych i rozrachunkach międzybankowych w III kwartale 2017 r., https://www.nbp. pl/systemplatniczy/publikacje/2017_3.pdf?v=20171023 (dostęp: 10.09.2018).

PwC. *Mobile Payment Report 2017*, https://www.pwc.de/mobilepayment (dostęp: 10.09.2018).

Statista.com. *Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018*.

2018. https://www.statista.com/statistics/522058/global-smartphone-fingerprintpenetration/ (dostęp: 10.09.2018).

Telesign, Lawless Research. *Beyond the Password: The Future of Account Security*. https://www.telesign.com/wp-content/uploads/2016/06/Telesign-ReportBeyondthePassword-June-2016-1. pdf (dostęp: 10.09.2018).

Thakkar, Danny. *Top Five Biometrics: Face, Fingerprint, Iris Palm, and Voice*. Ed. by bayometric.com. https://www.bayometric.com/biometricsface-finger-iris-palm-voice/ (dostęp: 10.09.2018).

TrendForce. *Penetracja rynkowa smartfonów z czujnikami linii papilarnych 2018*.

2018. https://press.trendforce.com/press/201801113049.html (dostęp: 10.09.2018).

Uryniuk J., *Ąlior*, *ING i SGB wycofują z oferty płatności mobilne NFC. Usługa będzie dostępna już tylko w dwóch bankach*, https://www.cashless. pl/wiadomosci/platnosci-mobilne/2174-alior-ing-isgb-wycofuja-z-oferty-platnosci-mobilne-nfc-uslugabedzie-dostepna-juz-tylko-w-dwoch-bankach (dostęp: 10.09.2018).

Visa – Digital Payments Study 2017. https://www.visa.pl/o-nas/ aktualnosci/upowszechnienie-pieniadza-mobilnego-wpolsce-77-percent-badanych-uzywa-smartfonow-dobankowania-i-codziennych-platnosci-2190949 (dostęp: 10.09.2018).

Visa. *Visa – Digital Payments Study 2017 ikonografika*. https://www.visa. pl/o-nas/aktualnosci/infografika-digital-paymentsstudy-2017-71231 (dostęp: 10.09.2018).

Visa. *European consumers ready to use biometrics for securing payments 2017*. https://www.visaeurope.com/newsroom/news/european-consumers-ready-for-biometrics (dostęp: 10.09.2018).