AUTORYZACJA BIOMETRYCZNA

WPROWADZENIE.

Kiedyś wyłącznie zakres kompetencji organów ścigania, wywiadu i agencji bezpieczeństwa narodowego, biometria - automatyczne rozpoznawanie ludzi na podstawie ich cech fizjologicznych lub behawioralnych - w końcu weszła do głównego nurtu biznesu jako metoda identyfikacji i uwierzytelniania dostępu do infrastruktury fizycznej i logicznej. . Kiedyś tylko marzenie, biometryczne technologie uwierzytelniania znacznie poprawiły bezpieczeństwo, wygodę i przenośność w porównaniu z innymi powszechnie stosowanymi metodami uwierzytelniania. Wskaźniki przyjęcia są nadal niższe, niż oczekiwali niektórzy specjaliści ds. Bezpieczeństwa; Jednak spadające koszty, ulepszenia technologii, zwiększone potrzeby w zakresie bezpieczeństwa i zmieniające się przepisy rządowe zachęcają do przyjęcia biometrii.

ZNACZENIE IDENTYFIKACJI I WERYFIKACJI.

Zapewnienie tożsamości i autentyczności osób jest warunkiem wstępnym bezpieczeństwa i skuteczności w dzisiejszych działaniach organizacyjnych. Intruzi mogą uszkodzić infrastrukturę fizyczną i logiczną, wykraść zastrzeżone informacje, zagrozić konkurencyjnym aktywom i trwałości organizacyjnej. Tradycyjne metody rozpoznawania i identyfikacji, w których jedna osoba identyfikuje drugą na podstawie głosu, wyglądu fizycznego lub chodu, są niepraktyczne, nieefektywne i niedokładne w zakresie współczesnych działań organizacyjnych. Aby sprostać zapotrzebowaniu na szybkie, wydajne i opłacalne uwierzytelnianie, organizacje obecnie polegają głównie na dwóch metodach „czegoś, co wiesz" i „czegoś, co masz" (stosowanych indywidualnie lub łącznie) w celu weryfikacji tożsamości osób uzyskujących dostęp ich fizyczną i / lub logiczną infrastrukturę. Najbardziej niezawodne systemy uwierzytelniania wykorzystują wiele czynników uwierzytelniania. Te formy uwierzytelnienia opisano w rozdziale 28 niniejszego podręcznika.

PODSTAWY I ZASTOSOWANIA.

Biometria opiera się na pomiarze i dopasowaniu charakterystycznych cech fizjologicznych i / lub behawioralnych. Te pierwsze opierają się na bezpośrednim pomiarze fizjologicznej charakterystyki jakiejś części ludzkiego ciała. Przykłady fizjologicznych danych biometrycznych obejmują skany palców, dłoni, siatkówki, twarzy i tęczówki. Te ostatnie pośrednio mierzą cechy ludzkiego ciała na podstawie pomiarów i danych pochodzących z działania. Powszechnie używane dane biometryczne behawioralne obejmują skanowanie głosu i sygnatur oraz wzorce naciśnięć klawiszy.

Przegląd i historia.

Stosowanie niezautomatyzowanych danych biometrycznych sięga początków ludzkiej cywilizacji, kiedy to jednostki zaczęły identyfikować inne osoby na podstawie pewnych cech fizycznych lub behawioralnych. Koncepcja biometrii jako środka uwierzytelniania sięga ponad 2000 lat wstecz. Już w 300 r. p.n.e. garncarze asyryjscy używali odcisku palca jako wczesnej formy identyfikacji marki dla swoich towarów. Stosowanie podpisów odręcznych (kotletów) w klasycznych Chinach to kolejny przykład wczesnej biometrii. W pierwszym przypadku formalnego, prawnego systemu uwierzytelniania biometrycznego, odciski palców były używane do podpisywania umów za panowania dynastii Tang (618–906). Rozwój współczesnych systemów biometrycznych można postrzegać jako wynik wysiłków naukowców kryminalistycznych i organów ścigania w celu zidentyfikowania i sklasyfikowania przestępców pod koniec XIX i na początku XX wieku. W 1882 roku Alphonse Bertillon wprowadził system pomiarów ciała zwany antropometrią w celu identyfikacji przestępców. Ten system okazał się niewiarygodny, ponieważ wykonane pomiary nie były unikalne w skali światowej. Uczeń Bertillona,

Edmund Locard, zaproponował później system odcisków palców oparty na pracy Sir Edmonda Galtona do identyfikacji ludzi poprzez analizę unikalnych punktów na grzbietach i porach odcisków palców. System Locarda, który wykorzystywał 12 punktów Galtona, jest do dziś uważany za niezawodny. Ta metodologia leży u podstaw w pełni zautomatyzowanej nowoczesnej biometrii, w tym zintegrowanych zautomatyzowanych systemów identyfikacji odcisków palców (IAFIS) używanych przez organy ścigania. Komercyjne systemy biometryczne (zazwyczaj opierające się na geometrii dłoni) zaprojektowane do użytku w fizycznym dostępie do budynków, pojawiły się w latach sześćdziesiątych i siedemdziesiątych XX wieku. Biometryczne metody identyfikacji i weryfikacji tożsamości, w tym automatyczna analiza odcisków palców i technologie rozpoznawania twarzy, były dostępne i stosowane przez niektóre agencje rządowe / publiczne (np. Organy ścigania, wywiad i bezpieczeństwo narodowe) oraz kilka branż prywatnych (np. Rozpoznawanie twarzy) skanów w kasynach) od lat 60. i 70. Niezależnie od potencjalnych korzyści i zalet w porównaniu z innymi metodami uwierzytelniania, biometria nie była szeroko stosowana, szczególnie w świecie korporacji. Analitycy wymieniają wysokie koszty sprzętu i wdrożenia, problemy technologiczne, słabe punkty określonych danych biometrycznych, brak standardów i opór użytkowników (zwłaszcza obawy o prywatność) jako przyczyny braku wdrożenia. Jednak od lat 90. XX wieku znaczące udoskonalenia technologii biometrycznych, ruch w kierunku standaryzacji, zmiany regulacyjne wymagające od organizacji przyjęcia rygorystycznych kontroli bezpieczeństwa i prywatności oraz znacznie obniżone koszty zachęciły do szerszego zastosowania. Szereg agencji rządowych Stanów Zjednoczonych (np. Departament Bezpieczeństwa Wewnętrznego, Departament Transportu, Departament Obrony, Ceł i Ochrony Granic, Departament Sprawiedliwości, Narodowa Biblioteka Medyczna) i firm w niektórych branżach (np. Służba zdrowia i finanse) znacznie zwiększył wykorzystanie danych biometrycznych w ciągu ostatnich kilku lat - jest to czynnik, który prawdopodobnie zachęci inne organizacje również do przyjęcia biometrii. HP i Lenovo oferują skanery linii papilarnych w swoich komputerach przenośnych, umożliwiając użytkownikom zwiększenie bezpieczeństwa, wymagając przesunięcia palca i hasła (lub po prostu przesunięcia palcem) w celu uzyskania dostępu do plików. Inni producenci komputerów i dostawcy urządzeń peryferyjnych dodali skanowanie odcisków palców do klawiatur komputerowych i / lub opracowali samodzielne skanery linii papilarnych, które łączą się z komputerami przez port uniwersalnej magistrali szeregowej (USB). Niektórzy analitycy postrzegają ataki z 2001 roku na World Trade Center i Pentagon również jako kluczowy bodziec do zwiększonego wykorzystania biometrii do uwierzytelniania i identyfikacji. Ataki terrorystyczne odegrały kluczową rolę w zachęcaniu do adopcji nie tylko dlatego, że zwiększyły obawy firm i agencji o bezpieczeństwo, ale także dlatego, że wpływ i konsekwencje ataków terrorystycznych zdają się obniżyć odporność użytkowników na wykorzystywanie biometrii przez pracodawców i rząd . Innymi słowy, w ten sam sposób, w jaki zagrożenie globalnym terroryzmem zmniejszyło sprzeciw opinii publicznej wobec możliwych naruszeń swobód obywatelskich w wyniku wdrożenia amerykańskiej ustawy PATRIOT Act i innych środków związanych z bezpieczeństwem, wydaje się, że ataki te spowodowały, że wiele osób straciło wrażliwe na potencjalne konsekwencje biometrii, które naruszają prywatność. Boroshok poinformował w 2007 r., Że ankieta sponsorowana przez AuthenTec wykazała, że 71 procent konsumentów w USA zapłaciłoby więcej za opcje zabezpieczeń biometrycznych w swoich telefonach komórkowych, a 63 procent konsumentów zapłaciłoby dodatkowy koszt za dodanie tych opcji do ich komputerów osobistych. Zmieniające się środowisko bezpieczeństwa wywołało prognozy szybkiego wzrostu biometrii. W 2004 roku Międzynarodowa Grupa Biometryczna (IBG) przewidziała szybki wzrost branży biometrycznej w ciągu następnych kilku lat, od przychodów w wysokości poniżej 50 mln USD w 2004 r. Do prawie 200 mln USD w 2008 r.2 Pod koniec 2003 r. Analitycy z San Jose w Kalifornii - firma badawcza Frost and Sullivan z siedzibą w USA przewidywała, że aplikacje biometryczne z aplikacji komercyjnych (z wyłączeniem IAFIS Federalnego Biura Śledczego) wzrosną z 93,4 mln USD w 2001 r. Do 2,05 mld USD w 2006 r. - z 700 mln USD (w 2006 r.) przewidywane przed atakami z 11 września 2001 roku. W styczniu 2009 roku IBG opublikowało swoje najnowsze prognozy wzrostu rynku

dla branży biometrycznej. Oszacowali, że przychody branży biometrycznej wzrosną z 3,01 mln USD w 2007 r. Do ponad 7,4 mln USD w 2012 r.3 Jest to dalekie od ich początkowej przewidywanej stopy wzrostu opublikowanej w 2004 r. I można ją przypisać brakowi standardów, kwestiom regulacyjnym i grupom zajmującym się prywatnością. który potępił naruszenie ich prywatności przez te urządzenia (IBG nie opublikował publicznie nowszego raportu, więc nie możemy stwierdzić, czy te prognozy zostały spełnione). Pomimo różowych prognoz analityków branżowych, wdrażanie systemów uwierzytelniania biometrycznego nadal pozostaje w tyle. Niektóre firmy nadal powołują się na kwestie związane z kosztami (chociaż te maleją) i obawy dotyczące prywatności, podczas gdy inne wskazują na problemy związane z wdrażaniem biometrii na lotniskach i wśród agencji rządowych. Ogólnie rzecz biorąc, badania firm wskazują, że prognozy dotyczące dramatycznego i szybkiego wzrostu we wdrażaniu biometrii mogą być zawyżone. Potwierdza to niedawne badanie priorytetów wydatków z 2013 r. Opublikowane przez InformationWeek. Spośród 513 firm, które odpowiedziały na ankietę, 13 procent zmniejszyło budżet w stosunku do budżetów na 2012 rok, a 43 procent nie zmieniło swoich budżetów - dla wielu jest to mentalność „rób, co możesz, mając to, co masz". Jednak mimo to 58 procent ankietowanych chciało ogólnie poprawić swoje bezpieczeństwo. Jednak w innym badaniu przeprowadzonym w 2013 r. Ankieta „Strategic Security Survey" przeprowadzona przez InformationWeek ujawniła, że 52 procent z ponad 1000 respondentów chciało poprawić swoje praktyki zarządzania tożsamością i hasłami. Pozorne rozłączenie można przypisać kierownictwu, które chce obniżyć koszty, oraz stale zmieniającemu się światowi przepisów - wielu czeka, aby zobaczyć, jak będzie wyglądał krajobraz, gdy opadnie kurz. Ankieta przeprowadzona przez Forrester Research z 2003 r. Wykazała, że tylko 1% firm wdrożyło systemy biometryczne, tylko 3% miało w toku wdrażanie systemów biometrycznych, tylko 15% testowało dane biometryczne, a 58% ankietowanych nie planowało ich wypróbować. Dziesięć lat później nadal nie widzimy żadnego istotnego przyjęcia uwierzytelniania biometrycznego.

Właściwości biometrii.

Współczesne znaczenie biometrii podkreśla jej zautomatyzowane aspekty, które pozwalają na wdrażanie na dużą skalę. Najczęściej cytowaną definicją biometrii jest pewna odmiana „automatycznej identyfikacji osoby na podstawie jej cech fizjologicznych lub behawioralnych". Termin „biometria" jest generalnie używany jako rzeczownik w odniesieniu do automatycznego rozpoznawania osób na podstawie ich cech fizycznych lub behawioralnych. Termin „biometryczny" może być używany jako rzeczownik w odniesieniu do pojedynczej technologii lub środka (np. Skan palca jest powszechnie stosowaną metodą biometryczną) lub jako przymiotnik, tak jak w przypadku „systemu biometrycznego wykorzystującego zintegrowany sprzęt i oprogramowanie do przeprowadzania identyfikacji lub weryfikacja." Biometria od dawna jest reklamowana jako możliwe rozwiązanie problemów i luk w zabezpieczeniach innych powszechnie stosowanych metod uwierzytelniania i identyfikacji. Reprezentują wyrafinowane wersje tradycyjnych środków identyfikacji, takich jak osłona umożliwiająca dostęp do użytkownika, którego strażnik rozpoznaje na podstawie wzroku. Biometrię powszechnie definiuje się jako zautomatyzowane metody rozpoznawania / weryfikacji / identyfikacji osób w oparciu o pewne mierzalne cechy fizjologiczne lub behawioralne, takie jak odciski palców, geometria dłoni, kształt twarzy, wzór tęczówki, głos, podpis i tym podobne. Podczas gdy identyfikatory (ID) i klucze uwierzytelniają użytkownika na podstawie tego, co posiada użytkownik, a hasła / osobiste numery identyfikacyjne (PIN) uwierzytelniają użytkownika na podstawie tego, co wie użytkownik, biometria umożliwia uwierzytelnianie i weryfikację tożsamości na podstawie tego, kim jest użytkownik. Ponieważ biometryczne metodologie uwierzytelniania faktycznie opierają identyfikację na fizjologicznych lub behawioralnych „elementach" użytkownika, biometria stanowi jedyną formę uwierzytelnienia, która bezpośrednio uwierzytelnia użytkownika. Biometria ma wiele innych oczywistych zalet w porównaniu z innymi powszechnie używanymi metodami uwierzytelniania. W

przeciwieństwie do identyfikatora lub klucza USB, nie można łatwo zgubić lub zgubić odcisku palca lub innych środków biometrycznych. Podobnie, w przeciwieństwie do przypadku z haseł i PIN-ów, nie trzeba pamiętać i nie można zapomnieć o jakiejś fizjologicznej lub behawioralnej charakterystyce. Chociaż środki biometryczne mogą być zagrożone, generalnie biometria jest znacznie trudniejsza do manipulowania poprzez kradzież, fałszowanie, udostępnianie lub niszczenie niż inne powszechnie używane narzędzia uwierzytelniania. Biometria zapewnia również sporą wygodę, w przeciwieństwie do kłopotów z zapamiętywaniem dziesiątek haseł. Chociaż początkowe koszty są dość wysokie, wdrożenie systemów biometrycznych zwykle skutkuje znacznie niższymi kosztami administracyjnymi niż inne metody dostępu ze względu na mniejszą liczbę wezwań do działu pomocy technicznej w celu zresetowania haseł, brak konieczności wydawania zastępczych identyfikatorów itd. Z tych i innych powodów biometria jest postrzegana jako zapewniająca lepsze bezpieczeństwo, zwiększoną wydajność i bardziej wiarygodne zabezpieczenie tożsamości niż inne powszechnie stosowane metody uwierzytelniania / identyfikacji oparte na tym, co posiada użytkownik lub co wie. Teoretycznie prawie każda cecha fizjologiczna i / lub behawioralna człowieka może być wykorzystana jako miara biometryczna. Jednak, aby zmieścić się w realnym, potencjalnie dokładnym i praktycznym systemie biometrycznym, używana biometria powinna również spełniać cztery inne wymagania oferowane przez Jaina i Bolle, Connell, Pankanti, Ratha i Seniora:

1. Uniwersalność. Każda osoba powinna mieć cechę biometryczną.

2. Wyjątkowość. Żadne dwie osoby nie powinny być takie same pod względem cech biometrycznych. Jain zaproponował nieco niższy standard charakteru odróżniającego, zdefiniowany jako „dwie dowolne osoby byłyby wystarczająco różne pod względem cechy".

3. Trwałość. Dane biometryczne powinny być stosunkowo niezmienne przez dłuższy okres czasu.

4. Kolekcjonalność. Charakterystyka biometryczna powinna nadawać się do pomiaru ilościowego w praktyczny sposób.

Bolle, Connell, Pankanti, Ratha i Senior argumentowali, że biometria powinna mieć również piąty atrybut: akceptowalność, definiowana jako „konkretna populacja użytkowników i ogół społeczeństwa nie powinien mieć poważnych zastrzeżeń co do pomiaru / gromadzenia danych biometrycznych". Jain argumentował, że praktyczny system biometryczny powinien uwzględniać dwa inne

atrybuty: (1) wydajność, czyli „osiągalna dokładność i szybkość rozpoznawania, zasoby wymagane do osiągnięcia pożądanej wydajności, a także czynniki operacyjne i środowiskowe, które mają wpływ na wydajność" oraz (2) obejście, które „odzwierciedla sposób system można łatwo oszukać przy użyciu oszukańczych metod ". Wraz z tym tokiem myślenia odkrywamy, że eksplozja BYOD w miejscu pracy otwiera drogę do zarządzania tożsamością i dostępem. Wraz z przejęciem AuthenTec przez Apple w 2012 r., Przypuszczenia szły w parze z propozycją nowego mobilnego urządzenia biometrycznego do użytku wewnątrz i na zewnątrz przedsiębiorstwa. Podczas gdy era BYOD przyniosła atrybut „akceptowalności", koncepcja Jaina dotycząca właściwych czynników operacyjnych i środowiskowych wciąż istnieje - to, w jakim stopniu zostanie to zaakceptowane, zostanie określone przez to, jak dobrze można nimi zarządzać i scentralizować za pomocą systemów IAM.

Identyfikacja, weryfikacja i uwierzytelnienie.

Biometria może pełnić kilka ról związanych z identyfikacją i uwierzytelnianiem (więcej informacji na temat tych pojęć można znaleźć w rozdziale 28 niniejszego podręcznika). Role te są często powiązane z użyciem terminu uwierzytelnienie biometryczne, podczas gdy w rzeczywistości system wykorzystujący dane biometryczne może przeprowadzać identyfikację, weryfikację lub

uwierzytelnianie… lub ich połączenie. Aby uniknąć nieporozumień w używaniu terminów, ważne jest, aby rozróżnić różne sposoby wykorzystywania danych biometrycznych. Systemy identyfikacji odpowiadają na pytanie, za kogo się podajesz? Pozwalają na wybranie pojedynczego przedmiotu z możliwej grupy przedmiotów na podstawie prezentacji informacji identyfikujących. Systemy identyfikacyjne są często określane jako systemy 1: N (onet-N lub jeden do wielu), ponieważ informacje biometryczne podmiotu są porównywane z wieloma (N) rekordami w celu ustalenia, który z nich jest zgodny. Ten rodzaj systemu ma zastosowanie w wyszukiwaniu pozytywnego dopasowania (takiego jak rozpoznawanie twarzy, które można by wykonać na lotniskach lub stadionach w celu znalezienia terrorystów), ponieważ a także dopasowanie negatywne (mające na celu zapewnienie, że dane biometryczne danej osoby nie są obecne w bazie danych, np. uniemożliwianie ludziom zapisywania się więcej niż raz do programów świadczeń na dużą skalę). Ale identyfikacja biometryczna może również służyć jako wygodny substytut wprowadzania nazwy użytkownika lub przeciągnięcia karty w celu podania tożsamości do automatycznego systemu wprowadzania danych lub logicznego systemu kontroli dostępu. Systemy weryfikacji odpowiadają na pytanie: czy jesteś tym, za kogo się podajesz? Próbują dopasować podane informacje (hasła, identyfikatory tokenów lub dane biometryczne) z wcześniej zarejestrowanymi („zarejestrowanymi") danymi uwierzytelniającymi przechowywanymi w systemie; dopasowanie do próby jest wybierane przez określony identyfikator użytkownika (ID) przedstawiony przez podmiot. Biometryczne systemy weryfikacji są określane jako systemy 1: 1 (jeden do jednego), ponieważ chociaż mogą zawierać tysiące, a nawet miliony zapisów biometrycznych, „zawsze opierają się na tym, że dane biometryczne użytkownika są porównywane tylko z jego własnymi zarejestrowane dane biometryczne ". Zatem prezentacja informacji biometrycznych ma na celu potwierdzenie (lub uwierzytelnienie) prawdziwości roszczenia podmiotu do przedstawionej tożsamości. To, czy jeden z tych systemów biometrycznych kwalifikuje się jako system uwierzytelniania, zależy od implementacji. Biometryczny system weryfikacji, który łączy w pary identyfikator użytkownika w przypadku danych biometrycznych zawsze przeprowadza zarówno identyfikację, jak i uwierzytelnianie. W takim przypadku dane biometryczne są używane zamiast znanego hasła lub danych wyjściowych tokena uwierzytelniającego i mogą zwiększyć bezpieczeństwo, unikając niektórych luk w zabezpieczeniach, które są plagą innych danych uwierzytelniających. Z drugiej strony system identyfikacji biometrycznej nie zawsze przeprowadza uwierzytelnianie. Może również pełnić rolę systemu uwierzytelniania, jeśli zostaną przedstawione dodatkowe czynniki uwierzytelniające (takie jak kod PIN) w celu potwierdzenia, że dane biometryczne są rzeczywiście przedstawiane przez podmiot, który system identyfikuje jako powiązany z informacjami. Bez drugiej informacji potwierdzającej powiązanie użycie identyfikatora biometrycznego zastępuje prezentację innych identyfikatorów użytkownika (takich jak wpisywanie identyfikatora użytkownika) iw tym sensie nie dokonuje uwierzytelnienia. Można argumentować, że ponieważ dane biometryczne odnoszą się bezpośrednio do jakiejś części ciała podmiotu lub do obserwowalnych cech zachowania podmiotu, przedstawienie danych biometrycznych należy uznać za formę bezpośredniego uwierzytelnienia. Zgodnie z tą argumentacją, w taki sam sposób, w jaki ochroniarz rozpoznaje upoważnionych pracowników przy bramie w ramach kombinacji identyfikacji / uwierzytelniania, biometryczny system identyfikacji w pewnym sensie uwierzytelnia podmiot. Argument ten jednak przesłania luki, które mogą oznaczać oba podejścia: strażnik może zostać oszukany przez przebranie, może błędnie zidentyfikować rodzeństwo (zwłaszcza bliźniaki) lub po prostu przeoczyć wystarczająco podobną twarz. Podobnie, automatyczny system identyfikacji biometrycznej może dać się nabrać na sfałszowane dane uwierzytelniające, a także nie rozróżniać bardzo podobnych danych biometrycznych. Poleganie na pojedynczej prezentacji biometrycznej zarówno do identyfikacji, jak i niejawnego uwierzytelnienia jest z pewnością szybsze i wygodniejsze, ale może wiązać się z ryzykiem, które powinno zostać złagodzone przez drugi czynnik uwierzytelniania . Systemy identyfikacji biometrycznej są trudniejsze do zaprojektowania i wdrożenia niż systemy weryfikacyjne ze względu na rozbudowane możliwości

wyszukiwania biometrycznych baz danych. Ponadto systemy identyfikacyjne są bardziej podatne na błędy niż systemy weryfikacyjne, ponieważ trzeba przeprowadzić o wiele więcej dopasowań, które zwiększają możliwość popełnienia błędu. Systemy weryfikacji są ogólnie znacznie szybsze (często podejmują decyzję o dopasowaniu / braku dopasowania w czasie krótszym niż sekunda) i dokładniejsze niż systemy identyfikacyjne. Systemy weryfikacji, w przeciwieństwie do systemów identyfikacyjnych, przeważają w zastosowaniach sektora prywatnego, zwłaszcza w aplikacjach bezpieczeństwa komputerowego i sieciowego. Systemy weryfikacji dominują również w aplikacjach zaprojektowanych do uwierzytelniania praw dostępu do budynków i pomieszczeń, chociaż czasami systemy identyfikacji są również wdrażane w środowiskach o wysokim poziomie bezpieczeństwa. Systemy identyfikacji często znajdują się w zastosowaniach sektora publicznego, takich jak egzekwowanie prawa (np. Zwolnienie warunkowe i administracja więzienna, medycyna sądowa itp.), Programy pożytku publicznego na dużą skalę, wywiad i aplikacje związane z bezpieczeństwem narodowym.

Obszary zastosowań.

Chociaż istnieje wiele potencjalnych zastosowań biometrii, te podstawowe można podzielić na cztery kategorie: bezpieczeństwo systemów (systemy logicznego dostępu), dostęp do obiektów (systemy dostępu fizycznego), zapewnienie niepowtarzalności osób oraz systemy identyfikacji publicznej. Wspólną cechą tych czterech aplikacji jest to, że wszystkie opierają się na osobach zarejestrowanych w systemach.

Bezpieczeństwo (systemy dostępu logicznego).

Systemy dostępu logicznego „monitorują, ograniczają lub udzielają dostępu do danych lub informacji". Przykłady obejmują dostęp do komputera lub sieci lub dostęp do konta. W tych systemach dane biometryczne zastępują lub uzupełniają kody PIN, hasła i tokeny. Wielkość i wartość handlu elektronicznego oraz wartość wrażliwych i osobistych informacji transportowanych i / lub przechowywanych w sieciach i komputerach sprawiają, że wykorzystanie danych biometrycznych do zabezpieczenia dostępu logicznego jest o wiele silniejszym segmentem przemysłu niż zabezpieczenia fizyczne. Wykorzystanie technologii biometrycznych do logicznej kontroli dostępu jest wciąż w powijakach. Najczęstszym podejściem biometrycznym jest użycie czytników linii papilarnych z samodzielnym czytnikiem USB lub z czytnikiem wbudowanym w laptop. Producenci zaczynają wprowadzać układ Trusted Platform Module (TPM) do nowych laptopów, aby obsługiwać różnorodne aplikacje kryptograficzne. W połączeniu z urządzeniami biometrycznymi, takimi jak czytniki linii papilarnych, układ TPM umożliwia aplikacjom, takim jak BitLocker firmy Microsoft, stosowanie biometrycznej kontroli dostępu do zaszyfrowanych woluminów na dysku twardym. Takie technologie są wciąż na tyle nowe, że mogą mieć problemy z kompatybilnością wsteczną i wsparciem między producentami, ale oferują one obietnicę znacznie bezpieczniejszego dostępu logicznego.

Dostęp do obiektów (systemy dostępu fizycznego).

Systemy dostępu do obiektów „monitorują, ograniczają lub umożliwiają przemieszczanie się osoby lub obiektu do lub z określonego obszaru". W tych systemach dane biometryczne zastępują lub uzupełniają klucze, karty dostępu lub karty bezpieczeństwa, umożliwiając upoważnionym użytkownikom dostęp do pokoi, skarbców i innych bezpiecznych obszarów. Systemy dostępu fizycznego są często wdrażane w głównych miejscach infrastruktury publicznej, takich jak lotniska, punkty kontroli bezpieczeństwa i obiekty graniczne, w celu monitorowania i ograniczania ruchu osób nieupoważnionych lub podejrzanych. Oprócz wejścia do bezpiecznych pomieszczeń, fizyczne systemy dostępu, gdy są stosowane w warunkach biznesowych, obejmują systemy rejestracji czasu pracy, łącząc dostęp do lokalizacji z audytem, kiedy nastąpiło uwierzytelnienie. Technologie biometryczne są wykorzystywane do fizycznej kontroli dostępu od jakiegoś czasu, ale nadal reprezentują szereg możliwych wdrożeń, od

samodzielnych zamków drzwi z czytnikiem linii papilarnych po kompletne systemy z centralnym przechowywaniem szablonów biometrycznych, rejestrowaniem i zabezpieczeniem przed awarią zasilania. Wybór systemu z tak szerokiej gamy produktów musi pasować do ogólnego stanu bezpieczeństwa obiektu, szczególnie w odniesieniu do przechowywania szablonów. Na przykład w prostym autonomicznym systemie drzwi szablony odcisków palców byłyby przechowywane w urządzeniu blokującym lub w jego pobliżu, a system mógłby nie mieć żadnych funkcji rejestrowania. O ile nie są połączone z alarmami nadzoru i włamań przewidującymi fizyczne zagrożenie, urządzenia te są bardziej odpowiednie do zastosowań o niższym poziomie bezpieczeństwa, takich jak magazyny, w których dostęp do klucza fizycznego może nie zapobiegać kradzieży. Systemy połączone centralnie oferują jednak lepszą integrację z ogólnym monitorowaniem i kontrolą dostępu, ale cierpią z powodu problemów z komunikacją i zasilaniem podczas przesyłania szablonów przez sieć. Wybór produktu, który dobrze współdziała z innymi częściami ogólnego systemu kontroli dostępu, ma kluczowe znaczenie.

Zapewnienie niepowtarzalności osób.

Wyjątkowość systemów identyfikacji biometrycznej zazwyczaj koncentruje się na zapobieganiu podwójnemu zapisowi do programów lub aplikacji, takich jak program świadczeń socjalnych. Główne zastosowanie tej aplikacji występuje w sektorze publicznym, chociaż podobne systemy mogłyby zostać wdrożone, aby zapobiec podwójnemu zapisaniu się do programów świadczeń pracowniczych.

Publiczne systemy identyfikacji.

Ostatnim zastosowaniem notatek biometrycznych jest ich użycie do identyfikacji przestępców i / lub terrorystów. Przestępcy i terroryści mogą nosić przebrania, zdobywać fałszywe dokumenty i zmieniać swoje nazwiska, ale dane biometryczne są dość trudne do podrobienia. W 2004 roku Departament Obrony Stanów Zjednoczonych uruchomił zautomatyzowany system identyfikacji biometrycznej (ABIS), który gromadzi dane biometryczne irackich powstańców w sposób zgodny z IAFIS. Pozwala to na identyfikację znanych recydywistów i osób chcianych. Żołnierze używają również Biometric AutomatedToolset (BAT) opracowanego przez Biuro Technologii Językowej Armii w celu identyfikacji osób na miejscu zamachów bombowych. Każdy, kto przebywa na tym obszarze, może uzyskać odnośniki do istniejącej bazy danych powstańców. BAT jest również używany do rejestrowania i identyfikowania członków armii irackiej. Chociaż systemy biometryczne są bardzo obiecujące, ważne jest również, aby zrozumieć, że nadal istnieją ograniczenia obecnej technologii, ale wraz z pojawieniem się nanotechnologii wiele z nich jest szybko przezwyciężanych.

Gromadzenie i prezentacja danych.

Jak wyjaśnia Jain, „System biometryczny to zasadniczo system rozpoznawania wzorców, który działa na zasadzie pozyskiwania danych biometrycznych od osoby, wyodrębniania zestawu funkcji z uzyskanych danych i porównywania tego zestawu funkcji z szablonem ustawionym w bazie danych". Punktem wyjścia dla systemu biometrycznego jest rejestracja: dane biometryczne użytkownika są początkowo gromadzone i przetwarzane w szablonie, w formie, w której są następnie przechowywane do dalszego użytku. Jak wyjaśniają Woodward, Orlans i Higgins: „Szablony nie są nieprzetworzonymi danymi ani zeskanowanymi obrazami próbki biometrycznej, ale raczej zbiorem charakterystycznych cech wyodrębnionych przez system biometryczny". Liu i Silverman opisują szablon jako „matematyczną reprezentację danych biometrycznych. Szablon może mieć różną wielkość od 9 bajtów w przypadku geometrii dłoni do kilku tysięcy bajtów w przypadku rozpoznawania twarzy ". Szablony są zastrzeżone dla każdego dostawcy i technologii z niewielką lub żadną interoperacyjnością między systemami. Ten brak interoperacyjności jest atrakcyjny z punktu widzenia prywatności, ale nieatrakcyjny z punktu widzenia opłacalności i potencjalnego wykonawcy, który jest zaniepokojony

przeznaczeniem znacznych inwestycji w pojedynczą niestandaryzowaną technologię. Termin „prezentacja" odnosi się do procesu, w którym użytkownik dostarcza dane biometryczne do urządzenia rejestrującego, patrząc w kierunku kamery, kładąc palec na podkładce lub czujniku lub wykonując inne określone badanie fizjologiczne. W celu weryfikacji lub identyfikacji użytkownik przedstawia dane biometryczne, które są następnie przetwarzane i konwertowane do szablonu. Ten szablon jest wyodrębnieniem charakterystycznych cech i nie jest odpowiedni do rekonstrukcji oryginalnych danych biometrycznych. Zeskanowany szablon jest następnie porównywany z zapisanymi szablonami rejestracji. Za każdym razem, gdy użytkownik tworzy prezentację, tworzony jest i dopasowywany nowy szablon. Należy zauważyć, zwłaszcza z punktu widzenia kwestii prywatności, że systemy biometryczne nie przechowują surowych danych biometrycznych; zamiast tego wykorzystują dane do tworzenia szablonów iw większości przypadków odrzucają dane biometryczne. Decyzje o dopasowaniu / braku dopasowania w systemie biometrycznym opierają się na punktacji, która jest „liczbą wskazującą stopień podobieństwa lub korelacji wynikający z porównania szablonów rejestracji i weryfikacji". 20 Podobnie jak szablony, system punktacji opiera się na zastrzeżonych algorytmy; nie ma standardowego systemu.

RODZAJE TECHNOLOGII BIOMETRYCZNYCH.

Jak wspomniano wcześniej, dane biometryczne można ogólnie podzielić na dwie kategorie: fizjologiczną i behawioralną. Międzynarodowa Grupa Biometryczna dostarcza danych dotyczących porównawczego udziału w rynku różnych technologii biometrycznych. Dane IBG koncentrują się na udziale w rynku z zastosowań komercyjnych i rządowych. Wszystkie osiem najlepszych technologii biometrycznych należy do kategorii fizjologicznej. Pięć z tych danych biometrycznych omówiono szczegółowo w następnych sekcjach.

Skanowanie odcisków palców.

Technologia skanowania odcisków palców lub linii papilarnych jest zdecydowanie najpowszechniej stosowaną technologią biometryczną. Status numer jeden skanowania odcisków palców jako biometrii jest utrzymywany, nawet jeśli wykluczone jest szerokie stosowanie pobierania odcisków palców przez organy ścigania. Rodzaj pobierania odcisków palców stosowany w komercyjnych systemach biometrycznych różni się od tego używanego w egzekwowaniu prawa. W większości dostępnych na rynku aplikacji biometrycznych stacja umożliwia skanowanie tylko jednego palca jednej ręki, podczas gdy organy ścigania często polegają na pełnych zestawach odcisków palców. Oprócz tego, że jest najczęściej używaną biometrią, pobieranie odcisków palców jest również jednym z najstarszych i najczęściej dobrze zbadane technologie biometryczne. Ponieważ jest to szeroko stosowana, dobrze udokumentowana i dojrzała technologia, koszty wdrożenia technologii opartych na skanach linii papilarnych są stosunkowo niskie. Ceny jednostkowe dla wersji stacji roboczej z powiązanym oprogramowaniem mogą wynosić nawet 150 USD; wersje serwerowe kosztują obecnie zaledwie 50 USD za sztukę. Zalety skanowania odcisków palców są jednym z głównych powodów jego popularności i obejmują:

* Szerokie zastosowanie.

* Dojrzała technologia.

* Niska cena.

* Wysoka łatwość obsługi. (Aby umieścić palec na * opuszce palca, potrzeba bardzo niewielkiego treningu).

* Ergonomiczny styl. (Wygodny w użyciu dla większości użytkowników.)

* Niska liczba błędów. (Wskaźniki fałszywego dopasowania są niezwykle niskie; współczynnik błędów krzyżowania jest niższy niż w przypadku skanowania głosu i rozpoznawania twarzy, wyższy niż w przypadku geometrii dłoni i skanowania tęczówki).

* Szybkie czasy transakcji. (W większości systemów uwierzytelnianie zajmuje mniej niż sekundę).

* Zdolność do wdrożenia w szerokim zakresie środowisk (np. Na stacjach roboczych, w drzwiach, wewnątrz / na zewnątrz).

* Możliwość zwiększania poziomów dokładności poprzez rejestrację wielu palców.

* Oprócz weryfikacji może zapewnić identyfikację z wysokim poziomem dokładności (jeśli jest odpowiednio skonfigurowana do uwzględniania wielu zapisanych palców).

Pomimo wielu zalet skanowanie odcisków palców nie jest pozbawione istotnych słabości. Jak zauważają Chirillo i Blaul, niektóre słabości tej technologii wynikają z tych samych czynników, które nadają jej mocne strony. „Ponieważ technologia odcisków palców jest jedną z najstarszych i najbardziej znanych technologii, publicznie dostępna jest duża ilość informacji o tym, jak ją pokonać". 21 Istnieje wiele sposobów udaremnienia skanów palców i uzyskania fałszywego dopasowania (fałszywa akceptacja) , w tym użycie manekina palca wykonanego z lateksu lub innego materiału, manipulacja skanerem w celu podniesienia utajonego odcisku osoby, która wcześniej korzystała ze skanera, a nawet użycie rzeczywistego palca, który nie jest już przymocowany do ciała . (Większość skanerów linii papilarnych nie jest w stanie odróżnić tkanki żywej od martwej). Z powodu tych czynników poziom bezpieczeństwa skanów odcisków palców nie jest w rzeczywistości tak imponujący, jak zdają się wskazywać niskie wskaźniki błędów. Należy zauważyć, że można by podjąć środki zaradcze w celu przezwyciężenia podatności skanów palców na oszustwa. Na przykład zarejestrowanie dodatkowych palców utrudnia oszustwa. Aby zmniejszyć ryzyko, że system zostanie udaremniony przez palce syntetyczne lub rozczłonkowane, do czujników można dodać skanery termiczne i / lub wilgoci, które wykrywają temperaturę palców i poziom wilgoci, które wskazywałyby na żywotność palca. Inne słabości to:

* Skaner wymaga częstej konserwacji, ponieważ ekrany / czujniki mają tendencję do zatrzymywania utrudniającego gromadzenia się tłuszczu ze skóry użytkownika i pozostałości.

* Wydajność może z czasem ulec pogorszeniu, zarówno z powodu starzenia się użytkowników (i ścierania się końcówek palców), jak i z powodu konieczności konserwacji systemu.

* Dane biometryczne ze skanowania odcisków palców nie są oczywiście odpowiednie dla użytkowników z brakującymi rękami lub niepełnosprawnymi rękami.

* Poziom wydajności obniża się wśród użytkowników, którzy mają drżenie rąk, ponieważ prezentacja danych biometrycznych będzie zniekształcona.

* Poziom wydajności pogarsza się również, gdy palce użytkowników są albo przesuszone (do dokładnego odczytu potrzebna jest pewna ilość normalnego nawilżenia skóry), albo nadmiernie wilgotne lub tłuste (jak w wyniku zbyt dużej ilości balsamu do rąk).

* Istnieje niewielki, ale znaczący wskaźnik niepowodzeń w zapisach (FTE), nawet wśród populacji z rękami i bez niepełnosprawności. Wskaźnik EPC dla skanów palców szacuje się na 2 do 10 procent i jest przypisywany osobom z genetycznie niewyraźnymi odciskami, bliznami na palcach, suchą skórą i odciskami palców zniszczonymi przez wiek i / lub pracę fizyczną.

Być może największa słabość skanowania odcisków palców nie ma jednak nic wspólnego z dokładnością i niezawodnością technologii. Zamiast tego odnosi się do akceptacji użytkownika. Ze względu na powiązanie skanów odcisków palców z egzekwowaniem prawa i przestępczością, często takie skany nie są łatwo akceptowane przez użytkowników, którym nie podoba się „skażenie" technologii w zastosowaniach kryminalistycznych i którzy mogą martwić się, że dane biometryczne ze skanów palców zostaną wykorzystane do innych celów. Według Chirillo i Blaula „Innym powodem, dla którego technologia odcisków palców nie jest powszechnie akceptowana, jest to, że może wymagać, aby poszczególne osoby korzystały z tego samego urządzenia, którego dotykają inni".

Skan / rozpoznanie twarzy.

Bolle, Connell, Pankanti, Ratha i Senior zauważają, że „wygląd twarzy jest szczególnie interesującą metodą biometryczną, ponieważ jest używany codziennie przez prawie wszystkich jako podstawowy sposób rozpoznawania innych ludzi. Ze względu na swoją naturalność rozpoznawanie twarzy jest bardziej akceptowalne niż inne dane biometryczne ". Jednak akceptacja przez użytkowników skanów twarzy znacznie spada, gdy użytkownicy odkryją, że były one używane w ukryciu. Jak zauważa Imparato: „Ze wszystkich technologii biometrycznych obecnie w użyciu rozpoznawanie twarzy jest prawdopodobnie najbardziej kontrowersyjne ". Podobnie jak w przypadku skanów palców, rozpoznawanie twarzy opiera się na identyfikacji nieznanych obrazów twarzy poprzez porównanie z bazą danych (znanych) szablonów twarzy. Rozpoznawanie twarzy jest używane jawnie w kontroli dostępu, gdzie jest używane do identyfikacji jeden do jednego. Ta aplikacja zapewnia stosunkowo wysoką wydajność, ponieważ środowisko jest ściśle kontrolowane, a dane wejściowe są przewidywalne. Rozpoznawanie twarzy może być również wykorzystywane w ukryciu w inwigilacji, gdzie służy do lokalizowania ludzi w tłumie (od jednego do wielu), aczkolwiek z różnymi rezultatami. Na przykład miasto Virginia Beach w stanie Wirginia od ponad pięciu lat stosuje system rozpoznawania twarzy do identyfikacji znanych (wcześniej zarejestrowanych) przestępców, ale nie zidentyfikował jeszcze ani jednego przestępcy. Dostępnych jest wiele technologii rozpoznawania twarzy, od pojedynczego obrazu, sekwencji wideo, obrazu trójwymiarowego, bliskiej podczerwieni po termogramy twarzy. Rozpoznawanie twarzy oferuje następujące korzyści:

* Ma możliwość wykorzystania istniejącego sprzętu do pozyskiwania obrazów, takiego jak aparaty cyfrowe, Internet, wideo i tym podobne.

* Ponieważ rozpoznawanie twarzy jest technologią opartą na oprogramowaniu, często nie ma potrzeby kupowania nowego sprzętu, zwłaszcza biorąc pod uwagę liczbę powszechnie stosowanych kamer telewizji przemysłowej (CCTV) i kamer monitorujących.

* Brak konieczności posiadania specjalistycznego sprzętu może pomóc w obniżeniu kosztów tej technologii, zakładając, że wysokie koszty oprogramowania nie równoważą oszczędności sprzętu.

* Jest to jedyna biometria umożliwiająca identyfikację na odległość bez współpracy lub nawet świadomości podmiotu.

* Jest łatwy w użyciu. Wystarczy, że użytkownik (lub cel) spojrzy na kamerę.

* Nie wymaga od użytkownika dotykania żadnego urządzenia (poważny sprzeciw dla niektórych użytkowników skanujących odciski palców i skany dłoni).

* Po wdrożeniu w sytuacjach weryfikacyjnych, skany twarzy mają wyjątkowo niski współczynnik niepowodzeń rejestracji. (W przeciwieństwie do odcisków palców ludzkie twarze są prawie zawsze charakterystyczne).

* Są w stanie rejestrować statyczne obrazy (np. Fotografie na prawach jazdy), co umożliwia realizację rejestracji na bardzo dużą skalę przy stosunkowo niskich kosztach i w krótkim czasie.

Systemy rozpoznawania twarzy mają również szereg poważnych słabości. Dominującą słabością (wynikającą z połączenia innych słabości technologii) jest niska dokładność i wysoki poziom błędów tej biometrii. Niezależnie od tego, czy jest stosowane potajemnie, czy jawnie, rozpoznawanie twarzy ma najniższy współczynnik dokładności spośród wszystkich pięciu najważniejszych biometrii. Odchylone głowy i niska rozdzielczość aparatu nadal zakłócają działanie programów, o czym świadczą zamachy bombowe w Bostonie w 2013 r.25 Dowody na niski współczynnik dokładności technologii pochodzą z badań przeprowadzonych na międzynarodowym lotnisku w Palm Beach (Floryda), które wykazały, że system zawiódł ponad 50% czas na dopasowanie 15 pracowników, którzy zarejestrowali się w bazie danych na okres próbny. Z 958 przejść system tylko 455 razy dopasował twarze pracowników. Niektóre badania sugerują, że można ulepszyć dokładność w systemach rozpoznawania twarzy, ale te ulepszenia będą się wiązać z bardzo wysokimi kosztami. Na przykład pakiet oprogramowania do rozpoznawania twarzy firmy Visionics FaceIt skutkował imponująco niskim poziomem błędów, o ile warunki oświetlenia były idealne. Oprogramowanie kosztuje 30 000 USD za system z trzema kamerami. Inne słabości to:

* Fałszywe dopasowania (fałszywe akceptacje) rutynowo występują w przypadku bliźniaków, a większość systemów jest na tyle niewrażliwa, że ktoś zręczny w maskowaniu i podszywaniu się pod inne osoby może skłonić system do fałszywego dopasowania.

* Bardziej prawdopodobne niż fałszywe dopasowania są jednak fałszywe niedopasowania (fałszywe odrzucenia), które mogą wystąpić w wyniku mimiki; zmiany fryzury, makijażu, zarostu, znaczące zmiany masy ciała, okularów i zmiany twarzy związane z wiekiem.

* Środowisko akwizycji może mieć ogromny wpływ na dokładność systemu rozpoznawania twarzy. W szczególności oświetlenie, zbyt jasne lub zbyt słabe, może znacznie zwiększyć współczynnik błędów.

* Dostrzegane zagrożenie prywatności. Jawnie stosowane technologie rozpoznawania twarzy (np. Wykorzystywane do identyfikacji i dostępu) są ogólnie oceniane jako stosunkowo dyskretne i spotykają się z wysokim poziomem akceptacji użytkowników. Jednak potajemnie rozmieszczone systemy, takie jak te używane do nadzoru, stanowią poważne zagrożenie dla prywatności. Zagrożenie to jest ogólnie postrzegane jako znacznie poważniejsze niż to stwarzane przez inne czołowe dane biometryczne.

Skanowanie geometrii dłoni.

Skany geometrii dłoni nie odnoszą się do odcisków dłoni ani do jakiejkolwiek analogii odcisków palców, ale raczej do struktury geometrycznej (lub niezmienników geometrycznych) ludzkiej dłoni. Nanavati, Thieme i Nanavati wyjaśniają, że „technologia skanowania dłoni wykorzystuje charakterystyczne aspekty dłoni - w szczególności wysokość i szerokość grzbietu dłoni oraz palców - w celu weryfikacji tożsamości osób". Wiodący producent sprzętu dla tej technologii, Recognition Systems, Inc. (RSI), posiada podstawowy skaner ręczny, który wykonuje 90 pomiarów od trzech do czterech rejestracji, aby stworzyć szablon użytkownika zawierający długość, szerokość i grubość oraz powierzchnię. dłoni i palców. Nowsze systemy zawierają mechanizmy wykrywania temperatury, aby zapewnić „żywe" obiekty. Wszystkie komponenty systemu skanowania ręcznego (sprzęt do akwizycji, odpowiednie oprogramowanie, komponenty pamięci masowej) znajdują się w samodzielnym urządzeniu. Skany dłoni są dobrze ugruntowaną technologią biometryczną (są w powszechnym użyciu od lat 70. XX wieku), ale w porównaniu z innymi wiodącymi metodami biometrycznymi, skany dłoni mają znacznie mniejszy zakres zastosowań. Skany dłoni służą wyłącznie do weryfikacji raczej niż do identyfikacji, ponieważ pomiary ręczne nie są wystarczająco charakterystyczne lub specyficzne, aby umożliwić

zastosowanie identyfikacji. Z tego powodu skanowanie dłoni jest używane głównie w przypadku dostępu fizycznego oraz aplikacji do pomiaru czasu i obecności. W tym drugim przypadku są one wykorzystywane jako sposób na wyeliminowanie problemu „dziurkowania koleżeńskiego", w wyniku którego jeden pracownik wbija lub atakuje nieobecnego współpracownika. Technologia skanowania ręcznego niewiele się zmieniła od czasu jej wprowadzenia ponad 30 lat temu, więc jej mocne i słabe strony są dobrze znane. Główne zalety skanowania dłoni to:

* Działa w bardzo trudnych warunkach. (Na sprzęt zwykle nie ma wpływu światło, kurz, wilgoć ani temperatura).

* Sprawdzona i niezawodna technologia.

* Łatwość użycia. (Użytkownicy po prostu wkładają rękę do urządzenia; umieszczenie ma niewielkie znaczenie).

* Odporność na oszustwa w porównaniu z innymi danymi biometrycznymi. (Zastąpienie fałszywej próbki byłoby trudne i czasochłonne).

* Mały rozmiar szablonu (zaledwie 9 bajtów; znacznie mniejszy niż w przypadku innych danych biometrycznych, co pozwala na przechowywanie tysięcy szablonów w jednej jednostce).

* W oparciu o stosunkowo stabilną charakterystykę fizjologiczną.

* Wysoki poziom akceptacji użytkowników i brak piętnowania.

Problemy zgłaszane podczas korzystania ze skanów dłoni obejmują:

* Ograniczona dokładność (co z kolei ogranicza jego użycie do weryfikacji, a nie identyfikacji). Stosunkowo niska dokładność skanu dłoni (wyższa niż rozpoznawanie twarzy i biometria behawioralna, ale niższa niż skany palców i tęczówki) jest wynikiem ogólnego braku różnorodności fizycznej wyrażanej w dłoni, a także stosunkowo niewielkiej liczby cech mierzonych skanem dłoni.

* Stosunkowo duży rozmiar (ogranicza to wdrażanie technologii w aplikacjach zorientowanych na komputer, które wymagają sprzętu o mniejszej powierzchni).

* Niektórzy ludzie czują się urażeni przymusowym kontaktem z prawdopodobnie nieczystymi powierzchniami.

* Ergonomiczna konstrukcja ogranicza jego użycie przez niektóre populacje (np. Osoby niepełnosprawne).

* Stosunkowo wysoki koszt. Podczas gdy koszt skanerów dłoni spadł do około 500 USD za model USB, skanery klasy korporacyjnej są nadal dość drogie, nawet przy wzroście liczby firm je produkujących.

Skanowanie tęczówki.

Technologia skanowania tęczówki wykorzystuje unikalny wzór utworzony przez tęczówkę - kolorową część oka ograniczoną źrenicą i twardówką - do identyfikacji lub weryfikacji tożsamości osób. Wzór tęczówki jest wyjątkowy, ponieważ nawet u tej samej osoby nie ma dwóch identycznych tęczówek. Wyjątkowość wzorów irysów została porównana do wielowarstwowych płatków śniegu. Patrząc z perspektywy, szansa pomylenia jednego wzoru tęczówki z innym wynosi 1 do 1078! Skany tęczówki osiągają to, umożliwiając porównanie ponad 200 punktów odniesienia, w przeciwieństwie do 60 do 70 używanych w odciskach palców. Unikalne aspekty tęczówki czynią ją idealnym materiałem biometrycznym do zastosowań o wysokim poziomie bezpieczeństwa; zapisanie obu tęczówek od tej samej osoby może zwiększyć poziom bezpieczeństwo. Oprócz aplikacji zapewniających dostęp fizyczny

o wysokim poziomie bezpieczeństwa, technologia skanowania tęczówki jest stosowana w bankomatach (bankomatach) i kioskach bankowych. Obecnie jest również używany w wydziałach policji w jednostkach podręcznych do identyfikacji podejrzanych i jest wprowadzany do takich zawodów, jak przejścia graniczne, i jest regularnie używany w Indiach, Iraku i Dubaju. Najważniejszą zaletą biometrii tęczówki jest jej dokładność, najważniejsza słabość skanowania twarzy. Spośród wszystkich wiodących biometrii technologia tęczówki ma najniższy poziom błędów i najwyższy poziom ogólnej dokładności. Inne mocne strony tej biometrii to:

* Możliwość wykorzystania zarówno do weryfikacji, jak i do identyfikacji.

* Stabilność jego cech biometrycznych przez całe życie.

* Względna trudność w sfałszowaniu lub podszywaniu się, ponieważ jest to wewnętrzna biometria.

* Fakt, że tęczówka jest w minimalnym stopniu narażona na wpływy zewnętrzne w porównaniu z danymi biometrycznymi, takimi jak odciski palców i twarze.

Główne słabości biometrii tęczówki dotyczą postrzegania przez użytkownika i problemów w interfejsie technologii użytkownika. Inne słabości to:

* Uzyskanie obrazu wymaga umiarkowanego treningu i uwagi: użytkownicy muszą stać nieruchomo i patrzeć prosto w skaner z otwartymi oczami i bez mrugnięcia.

* Użytkownicy często zgłaszają pewien dyskomfort fizyczny podczas korzystania z technologii opartej na oku, chociaż jest to mniejszy niż w przypadku technologii skanowania siatkówki.

* Anegdotyczne doniesienia sugerują również dość wysoki poziom odporności psychicznej użytkowników na technologię skanowania tęczówki, przy czym niektórzy użytkownicy uważają, że skaner doprowadzi do uszkodzenia oczu.

* Może niekorzystnie wpływać na oświetlenie i inne warunki środowiskowe (chociaż nie w zakresie skanowania twarzy).

* W niektórych przypadkach okulary niekorzystnie wpływają na wydajność (chociaż wiele urządzeń tęczówki może skanować osoby noszące okulary lub soczewki kontaktowe).

* Chociaż tęczówka jest względnie stabilną biometrią, wpływa na nią starzenie się i choroby.

* Opiera się na zastrzeżonych technologiach sprzętowych i programowych.

* Koszty wydają się być wysokie w porównaniu ze skanowaniem palców, skanowaniem dłoni i wieloma systemami rozpoznawania twarzy.

Z drugiej strony, koszt jednostkowy wiodącej technologii łączenia sprzętu i oprogramowania spadł do zaledwie 300 USD na stanowisko, wciąż wyższy niż w przypadku skanów odcisków palców, ale znacznie niższy niż cena ponad 5000 USD za stanowisko sprzed kilku lat.

Rozpoznawanie głosu.

Biometria rozpoznawania głosu „wykorzystuje charakterystyczne aspekty głosu do weryfikacji tożsamości osób". Rozpoznawanie głosu jest ogólnie klasyfikowane jako biometria behawioralna, chociaż w rzeczywistości łączy elementy biometrii behawioralnej i fizjologicznej: „Kształt przewodu głosowego determinuje w dużym stopniu to, jak brzmi głos, zachowanie użytkownika determinuje to, co jest mówione iw jaki sposób ". Mówiąc nieco inaczej, „głos jest behawioralną cechą biometryczną, ale zależy od podstawowych cech fizycznych, które regulują rodzaj sygnałów mowy, które jesteśmy w

stanie i prawdopodobnie wypowiemy". Ze względu na stosunkowo niski poziom dokładności i znaczną zmienność dynamiki głosu użytkowników, ta biometria jest zwykle używana tylko do weryfikacji, a nie do identyfikacji. Powszechnie stosowane systemy rozpoznawania głosu można podzielić na dwa typy: systemy zależne od tekstu (mówca jest proszony o powiedzenie określonej rzeczy) i systemy niezależne od tekstu (system uwierzytelniania przetwarza wszystkie wypowiedzi mówcy), które zapewniają wyższy poziom bezpieczeństwa, ponieważ są trudniejsze do podrobienia i zapewniają lepszą dokładność niż systemy zależne od tekstu. Mocne strony rozpoznawania głosu to:

* Możliwość wykorzystania istniejącej infrastruktury telefonicznej (a także wbudowanych mikrofonów komputerowych).

* Niski koszt, gdy używana jest istniejąca infrastruktura.

* Łatwość użycia.

* Interfejs z rozpoznawaniem mowy i hasłami werbalnymi.

* Wysoki poziom akceptacji użytkownika. (Ta biometria nie cierpi z powodu negatywnego postrzegania związanego z wszystkimi innymi wiodącymi biometriami).

Słabe strony rozpoznawania głosu obejmują:

* Bardziej podatny na ataki powtórkowe niż inne dane biometryczne.

* Poziomy dokładności są niskie w porównaniu ze skanowaniem tęczówki, skanami palców i skanami dłoni.

* Na poziom dokładności negatywnie wpływa hałas otoczenia i niska jakość urządzeń przechwytujących.

* Dokładność, bezpieczeństwo i niezawodność są kwestionowane przez indywidualne różnice w głosie, takie jak mówienie cicho lub głośno, chrypka lub nosowość z powodu przeziębienia itp.

* Na stabilność danych biometrycznych mają wpływ choroby, starzenie się i inne zachowania użytkowników, w tym palenie.

Inne technologie biometryczne.

Pięć głównych technologii biometrycznych, które właśnie omówiono łącznie, obejmuje zdecydowaną większość wdrażanych technologii biometrycznych. Inne technologie biometryczne, które rejestrują podziały udziałów w rynku, to dwie technologie behawioralne: skanowanie podpisów i skanowanie naciśnięć klawiszy. Chociaż obie te biometrie behawioralne są dobrze akceptowane (skanowanie podpisów bardziej niż skanowanie za pomocą klawiszy), ich przydatność jest ograniczona przez ich brak dokładności. Inne badane biometrie behawioralne obejmują chód i ruch warg. Jednym z fizjologicznych parametrów biometrycznych, którym poświęcono wiele uwagi ze względu na wysoką dokładność i wskaźniki bezpieczeństwa, jest skanowanie siatkówki. Jednak większość analityków uważa, że problemy związane ze skanowaniem siatkówki (brak akceptacji użytkownika, wysoki koszt, trudny i bolesny proces pozyskiwania) przeważają nad zaletami tej biometrii. Wydaje się, że konsensus jest taki, że skanowanie tęczówki zastąpiło skanowanie siatkówki jako wybraną biometrię skanowania oka. Wykorzystanie DNA jako identyfikatora biometrycznego również zostało zbadane, chociaż ma on znaczące słabości, w tym fakt, że DNA w tkankach ciała (np. Komórkach nabłonka) można potajemnie uzyskać i łatwo przenieść w niecnych celach, podczas gdy oficjalne metody pobierania (np. , pobieranie próbek krwi) są stosunkowo uciążliwe. Inne fizjologiczne parametry biometryczne, które mogą okazać się przydatne w przyszłości, obejmują zapach ciała, odbicie skóry i kształt ucha

RODZAJE BŁĘDÓW I MIERNIKI SYSTEMU.

We wszystkich typach systemów identyfikacji i uwierzytelniania występują dwa rodzaje błędów: fałszywe akceptacje i fałszywe odrzucenia.

Fałszywa akceptacja.

Znany również jako fałszywe dopasowanie, fałszywie dodatni lub błąd typu 1, fałszywa akceptacja to prawdopodobieństwo, wyrażone w procentach, że oszust zostanie dopasowany do danych biometrycznych prawidłowego użytkownika. W niektórych systemach, takich jak te, które próbują zabezpieczyć dostęp do obiektu zbrojeniowego, skarbca banku lub konta administratora systemu wysokiego poziomu, współczynnik fałszywego dopasowania / fałszywego akceptacji jest najważniejszą miarą, którą należy obserwować. W innych systemach, takich jak system rozpoznawania twarzy wdrożony przez kasyno w celu wykrycia liczników kart, może być tolerowany wysoki poziom fałszywych dopasowań.

Fałszywe odrzucenie.

Znany również jako fałszywy niedopasowanie, fałszywie negatywny lub błąd typu 2, fałszywe odrzucenie to prawdopodobieństwo, że „szablon użytkownika zostanie nieprawidłowo oceniony jako niezgodny z jego szablonem rejestracji". Fałszywe niedopasowania zazwyczaj powodują zablokowanie dostępu użytkownika do systemu. Te fałszywe niezgodności mogą wystąpić z powodu zmian w danych biometrycznych użytkownika, zmian w sposobie prezentacji danych biometrycznych i / lub zmian w środowisku. Systemy biometryczne są generalnie bardziej podatne na fałszywe odrzuty niż na fałszywe akceptacje.

Współczynnik błędów crossover.

Ważną miarą w systemach biometrycznych jest współczynnik błędu skrośnego (CER), znany również jako współczynnik równych błędów (EER). Ta użyteczna miara to punkt przecięcia fałszywych współczynników akceptacji i fałszywych odrzuceń. Ogólnie rzecz biorąc, niższy CER wskazuje, że urządzenie biometryczne jest dokładniejsze i bardziej niezawodne niż inne urządzenie biometryczne z wyższym CER. Rysunek 29.2 przedstawia podsumowanie dokładności / błędów opartych na testach porównawczych dla pięciu najbardziej rozpowszechnionych technologii biometrycznych. Każda technologia biometryczna jest uszeregowana w kolejności od najdokładniejszej do najmniej dokładnej na podstawie CER.

Brak rejestracji.

Inną krytyczną miarą w systemach biometrycznych jest FTE. Jak wyjaśnia Ashbourn, FTE odnosi się do „sytuacji, w której osoba nie jest w stanie zarejestrować swoich danych biometrycznych w celu stworzenia szablonu o odpowiedniej jakości do późniejszej zautomatyzowanej operacji". Typowe przyczyny niepowodzenia rejestracji obejmują niepełnosprawność fizyczną i użytkownika, którego cechy fizjologiczne / behawioralne są mniej wyraźne niż przeciętne. Nanavati, Thieme i Nanavati zauważają, że niepowodzenie w rejestracji może być poważnym problemem w „wewnętrznych wdrożeniach dla pracowników", w których „wysokie stawki FTE są bezpośrednio związane ze zwiększonym ryzykiem bezpieczeństwa i zwiększonymi kosztami systemu". Ostatnim ważnym wskaźnikiem jest „czas transakcji". Czas transakcji odnosi się do „teoretycznego czasu potrzebnego do dopasowania aktualnego szablonu do próbki referencyjnej".

WADY I PROBLEMY

Uwagi ogólne.

Pomimo wielu zalet w porównaniu z innymi powszechnie stosowanymi systemami uwierzytelniania, wdrożenie kontroli uwierzytelniania biometrycznego niesie ze sobą szereg zagrożeń i wad. Nawet najdokładniejszy system biometryczny nie jest doskonały i pojawią się błędy. Wskaźniki błędów i rodzaje błędów będą się różnić w zależności od zastosowanych konkretnych danych biometrycznych i okoliczności wdrożenia. Niektóre rodzaje błędów, takie jak fałszywe dopasowania, mogą stanowić fundamentalne, krytyczne zagrożenie dla bezpieczeństwa organizacji. Inne typy błędów - niepowodzenie rejestracji, fałszywa niezgodność - mogą zmniejszyć produktywność i wydajność organizacji oraz zwiększyć koszty. Organizacje planujące wdrożenie biometrii będą musiały wziąć pod uwagę dopuszczalny próg błędu. W każdym razie organizacje wdrażające systemy uwierzytelniania biometrycznego nie mogą dać się zwieść przekonaniu, że są odporne na błędy i / lub oszustwa. Niektóre systemy biometryczne (np. Skanowanie tęczówki oka) są dość odporne na oszustwa, podczas gdy inne (zwłaszcza systemy oparte na zachowaniu) są na nie znacznie bardziej podatne. Systemy skanowania twarzy można zafoliować ubraniem, makijażem, okularami i / lub zmianą fryzury. Nawet stosunkowo stabilne dane biometryczne oparte na fizjologii, takie jak skany odcisków palców, mogą zostać oszukane przy użyciu palców gumowych lub żelatynowych. Matsumoto przedstawia podejście gumowatego palca, mające na celu zmylenie nawet tych środków zaradczych. Zastosowane białko ma podobną reakcję galwaniczną na mięso, a ponieważ jest bardzo cienkie i przyczepione do żywego palca, ma odpowiednią temperaturę. W niektórych przypadkach nadmuch ciepłego powietrza na skaner może nawet spowodować utajnienie śladu poprzednika intruza. Wdrożenie powszechnie używanych systemów uwierzytelniania (tj. Identyfikatorów, haseł itp.) Wymaga stosunkowo niewielkiego szkolenia, chociaż można argumentować, że lepsze szkolenie w zakresie opracowywania i używania haseł poprawiłoby bezpieczeństwo. Ta ograniczona potrzeba szkolenia nie ma miejsca w przypadku większości najczęściej używanych systemów biometrycznych. Zarówno administratorzy systemów, jak i użytkownicy potrzebują instrukcji i szkolenia, aby zapewnić płynne działanie systemu. Niektóre systemy biometryczne są wyjątkowo wrażliwe na różnice w prezentacji i działaniu wewnątrz i między użytkownikami. Ich skuteczność jest znacznie zagrożona, a wskaźniki błędów znacznie wzrastają w przypadkach znacznych odchyleń i / lub nieprawidłowej prezentacji. Powiązany problem dotyczy akceptacji systemu biometrycznego przez użytkownika. Niektórzy użytkownicy mogą sprzeciwić się wdrożeniu danych biometrycznych ze względu na obawy dotyczące prywatności i ingerencji. W innych przypadkach użytkownicy mogą sprzeciwić się wdrożeniu biometrii i unikać optymalnego interfejsu z systemem ze względu na bezpieczeństwo i / lub zdrowie, ogólne obawy i / lub przekonania kulturowe i religijne. Na przykład niektóre osoby mogą obawiać się, że systemy biometryczne wymagające od nich dotykania opuszki palca lub podkładki pod dłonią niepotrzebnie narażą je na zarazki i narażą na ryzyko choroby. Niektórzy użytkownicy mogą obawiać się, że skanowanie oczu spowoduje uszkodzenie oczu. Inni użytkownicy mogą sprzeciwić się skanowaniu oczu na tej podstawie, że oczy są oknem duszy. Anderson zauważa, że niektóre osoby mogą sprzeciwić się używaniu danych biometrycznych z powodu osobistej interpretacji doktryny religijnej36. Niezależnie od przekonań użytkowników i ich opinii na temat systemu biometrycznego, w wielu przypadkach cechy lub elementy związane z użytkownikami i / lub środowiskiem operacyjnym będą wpływają na pomyślne wdrożenie i skuteczność systemu.

Względy dotyczące zdrowia i niepełnosprawności.

Osoby z zapaleniem stawów i / lub niektórymi innymi niepełnosprawnościami i ograniczeniami fizycznymi mogą nie być w stanie zapisać się do systemów, a następnie fizycznie ustawić się w optymalnej pozycji w odniesieniu do czujników biometrycznych. Na przykład użytkownicy z ciężkim zapaleniem stawów ręki mogą nie być w stanie mocno położyć ręki zgodnie z wymaganiami na czujniku geometrii dłoni, a użytkownicy z migrenami i związaną z nimi światłowstrętem mogą uznać, że patrzenie prosto w czujnik światła podczas skanowania tęczówki może być fizycznie zbyt niewygodne. Niektóre osoby niepełnosprawne mogą być całkowicie wykluczone z systemów biometrycznych.

Niektóre stosunkowo drobne ułomności, takie jak lekkie drżenie, mogą utrudniać dostęp legalnego użytkownika za pośrednictwem określonych systemów biometrycznych. Różnice w wielkości fizycznej mogą również wpływać na dokładność systemu. Skaner tęczówki ustawiony na standardową wysokość może nie przechwytywać obrazów bardzo niskich lub bardzo wysokich osób, aw niektórych przypadkach dłonie lub palce danej osoby mogą być zbyt duże lub zbyt małe, aby można je było dokładnie odczytać za pomocą skanera dłoni lub palca . Podobnie osobom z problemami z szyją i plecami może być trudno korzystać z niektórych urządzeń biometrycznych, w zależności od rodzaju wymaganego ustawienia. Systemy, które opierają się na biometrii behawioralnej, takiej jak głos lub podpis, są szczególnie podatne na zmiany i nieprawidłowości w cechach użytkownika. Na przykład użytkownicy, którzy mówią zbyt cicho, zbyt głośno lub zbyt szybko, mogą powodować błędy systemowe. Niewielkie zmiany w zdrowiu użytkowników mogą wpłynąć na niektóre odczyty biometryczne. Nadmierne nawilżenie skóry lub jej brak może mieć wpływ na skanowanie palców. Chociaż jedną z idealnych właściwości biometrii jest jej uniwersalność, w rzeczywistości nie każdy ma tę cechę lub ma ją w takim samym stopniu. Na przykład niektórzy ludzie rodzą się bez wyraźnych odcisków palców. W innych przypadkach użytkownicy mogli utracić charakter odróżniający swoich odcisków palców z powodu lat pracy fizycznej, stosowania niektórych chemikaliów, powstawania blizn lub procesu starzenia. Anderson zauważa, że „osoby o ciemnych oczach i dużych źrenicach dają gorsze kody tęczówki”. Niektóre choroby oczu i stany metaboliczne mogą również zmniejszać lub negować skuteczność uwierzytelniania na podstawie skanowania oczu. Wiek ma znaczący wpływ na interfejs użytkownika-systemu biometrycznego. Określone zmiany fizjologiczne są związane z procesem starzenia i mogą skutkować słabym dopasowaniem szablonu do żywej biometrii. W takim przypadku może być konieczna ponowna rejestracja. Proces starzenia wpływa na odciski palców, ponieważ skóra staje się bardziej sucha i krucha; wzorce głosu zmieniają się w jakości tonalnej w czasie; a kształt lub wygląd twarzy może zmieniać się z wiekiem. Ogólnie rzecz biorąc, akceptowalność systemu biometrycznego zostanie zmniejszona, jeśli powstanie wrażenie, że wdrożenie systemu dyskryminuje osoby niepełnosprawne, chorych, mniejszości etniczne, osoby starsze i inne osoby chronione lub znajdujące się w tradycyjnym niekorzystnym położeniu lub w inny sposób niekorzystnie na nie wpływa grupy użytkowników. Organizacje muszą zapewnić zgodność z amerykańską ustawą o niepełnosprawności przy wdrażaniu systemów uwierzytelniania biometrycznego. Zgodność może obejmować zapewnienie alternatywnych metod uwierzytelniania osobom, których to dotyczy.

Względy środowiskowe i kulturowe.

Szeroki wybór czynników środowiska operacyjnego mogą również wpływać na skuteczność i akceptowalność systemów biometrycznych. Czynniki kulturowe, społeczne i behawioralne związane z użytkownikiem mogą wpływać na wydajność systemu. Na przykład dokładność skanów twarzy może być zagrożona przez zmiany fryzury, zarostu i nakrycia głowy użytkownika, a także przez zmiany w wyglądzie fizycznym osoby z powodu znacznego przyrostu lub utraty wagi. Na dokładność systemów rozpoznawania głosu / mowy wpływa odległość między skanerem a użytkownikiem, a także głośność mowy. Rozpoznawanie odcisków palców jest utrudnione w przypadkach, gdy skóra użytkownika jest zbyt sucha, niezależnie od tego, czy stan jest wynikiem starzenia się, chorób skóry, czynników środowiskowych lub czynników związanych z wykonywaną pracą, takich jak częste mycie rąk wśród pracowników służby zdrowia. Na dokładność systemu biometrycznego mogą również wpływać czynniki w otaczającym środowisku otoczenia. Oświetlenie otoczenia wpłynie na dokładność i współczynnik błędów w skanach twarzy oraz, w mniejszym stopniu, na skanach tęczówki. Poziomy hałasu mogą osłabiać skuteczność systemów rozpoznawania głosu. Wilgotność i temperatura powietrza mogą wpływać na dokładność skanowania odcisków palców i dłoni.

Rozważania dotyczące kosztów.

Chociaż koszt wdrożenia systemu biometrycznego drastycznie spadł w ciągu ostatnich kilku lat, dla wielu organizacji nadal stanowi on poważną barierę. Koszty różnią się znacznie w zależności od rodzaju systemu. Ostatnie raporty sugerują, że nowsze skanery linii papilarnych można kupić już za 50 USD za sztukę; systemy rozpoznawania głosu mogą kosztować ponad 50 000 USD. Jednak nawet najtańsze systemy biometryczne prawdopodobnie będą kosztować więcej niż prostsze wersje tradycyjnych systemów uwierzytelniania. Eksperci szacują minimalne koszty, w tym sprzętu i oprogramowania, na około 200 USD na użytkownika i ponad 150 000 USD za ochronę całej firmy w średniej wielkości firmie. Problemem połączonym z kosztami są problemy związane z brakiem jasnych standardów i brakiem jasnej interoperacyjności między różnymi systemami uwierzytelniania biometrycznego. Wiele problemów i trudności związanych z systemami biometrycznymi prawdopodobnie zostanie skorygowanych lub znacznie złagodzonych dzięki udoskonaleniom technologicznym, lepszemu przeszkoleniu użytkowników i administratorów oraz dobrej kontroli warunków środowiskowych. W innych przypadkach problemy można przezwyciężyć lub złagodzić za pomocą środków zaradczych, takich jak łączenie różnych typów danych biometrycznych, łączenie danych biometrycznych z tradycyjnymi systemami uwierzytelniania i tak dalej. Dwa główne problemy, które nadal będą się pojawiać i zasługują na dokładniejsze zbadanie, to kradzież tożsamości biometrycznej i prywatność użytkownika.

Ataki na systemy biometryczne.

Chociaż dane biometryczne są znacznie mniej podatne na ataki niż inne metody uwierzytelniania, nie są odporne na oszustwa. Co więcej, kiedy tożsamość biometryczna zostanie skradziona lub sfałszowana, stwarza to znacznie większy problem niż ten spowodowany kradzieżą identyfikatora, klucza USB lub hasła, ponieważ danych biometrycznych nie można po prostu anulować i wymienić. Jedną z głównych zalet stosowania danych biometrycznych do uwierzytelniania jest ich niezmienność w czasie. W rezultacie, gdy oszust lub intruz oszukuje system uwierzytelniania biometrycznego i tworzy fałszywy błąd dopasowania, cały system bezpieczeństwa biometrycznego zostaje oszukany, a integralność biometryczna upoważnionego użytkownika zostaje naruszona. Podobnie Prabhakar, Pankanti i Jain zauważają: „Jedną z wad biometrii jest to, że nie można ich łatwo cofnąć. Jeśli dane biometryczne zostaną kiedykolwiek naruszone, zostaną utracone na zawsze ”. Wielu analityków uważa, że ostatecznym rozwiązaniem problemu kradzieży tożsamości biometrycznej jest opracowanie „danych biometrycznych z możliwością anulowania”. Badacze z IBM opracowali prototyp anulowalnego elementu biometrycznego, który zawiera powtarzalne zniekształcenie danych biometrycznych. Podobnie jak w teorii do stosowania kluczy publicznych i prywatnych do szyfrowania, przy każdej rejestracji wprowadzane jest unikalne zniekształcenie danych biometrycznych. Dlatego też, jeśli dane biometryczne użytkownika zostaną naruszone, oszukany zostanie tylko jeden system, a nie każdy system, w którym zarejestrowany jest użytkownik.

Kwestie prywatności.

Stosowanie kontroli uwierzytelniania biometrycznego budzi poważne obawy dotyczące prywatności, szczególnie w porównaniu z konwencjonalnymi metodami uwierzytelniania, takimi jak hasła i identyfikatory. Sprzeciwy użytkowników wobec danych biometrycznych często opierają się na obawach dotyczących prywatności, czasami wyrażanych w kategoriach poczucia użytkownika co do ingerencji systemu biometrycznego. Anegdotyczne raporty sugerują, że opinia publiczna na temat ingerencji różni się w zależności od różnych danych biometrycznych oraz sposobu ich wdrażania. W odniesieniu do tego ostatniego Nanavati, Thieme i Nanavati podają, że istnieje większe ryzyko naruszenia prywatności, gdy:

* Wdrożenie jest ukryte (użytkownicy nie są świadomi działania systemu) a nie jawne.

* System jest obowiązkowy, a nie opt-in.

* System służy raczej do identyfikacji niż weryfikacji.

* Jest wdrażany na czas nieokreślony w porównaniu z ustalonym czasem trwania.

* Jest wdrażany w sektorze publicznym i prywatnym.

* Użytkownik kontaktuje się z systemem jako pracownik / obywatel kontra osoba fizyczna / klient.

* Instytucja, a nie użytkownik, jest właścicielem informacji biometrycznych.

* Dane biometryczne są przechowywane w bazie danych szablonu, a nie w pamięci osobistej użytkownika.

* System przechowuje możliwe do zidentyfikowania dane biometryczne w porównaniu z szablonami.

Żywy przykład braku akceptacji opinii publicznej dla potajemnego wykorzystania systemów biometrycznych pochodzi z Super Bowl w 2001 r. I wrzawy, która nastąpiła po tym, jak Departament Policji w Tampa wdrożył technologię skanowania twarzy w celu wyłonienia podejrzanych z publiczności. W przeciwieństwie do tego, w następstwie ataków na World Trade Center i Pentagon w 2001 roku, na lotniskach w Stanach Zjednoczonych panowała dość powszechna akceptacja społeczna dla stosowania skanowania twarzy. Użytkownicy zazwyczaj postrzegają biometrię opartą na zachowaniu, taką jak rozpoznawanie głosu i weryfikacja podpisu, jako mniej inwazyjną i mniej zagrażającą prywatności niż opartą na fizjologii biometria. Uważa się, że skanowanie twarzy ma duży potencjał naruszenia prywatności ze względu na możliwość jego wdrożenia bez wiedzy i udziału użytkownika. Skany palców mogą być postrzegane jako inwazyjne i naruszające prywatność ze względu na ich związek z funkcjami organów ścigania. Poziom inwazyjności skanowania.

Wydaje się, że technika wpływa na postrzeganie przez użytkowników naruszenia prywatności, a skanowanie tęczówki wywołuje więcej zastrzeżeń do prywatności niż skanowanie ręczne. Obywatelscy libertarianie i użytkownicy również zgłaszają zastrzeżenia dotyczące prywatności w stosunku do systemów biometrycznych, które mogą ujawnić dodatkowe informacje o użytkowniku poza tożsamością biometryczną. Na przykład skany palców, ze względu na możliwość połączenia ich z dużymi bazami danych odcisków palców organów ścigania, mogłyby zostać wykorzystane do ujawnienia informacji o przeszłości kryminalnej użytkownika. Skany tęczówki mogą ujawnić poufne informacje medyczne / zdrowotne dotyczące użytkownika. Prawdopodobnie jednym z najbardziej niepokojących aspektów biometrii związanych z prywatnością jest możliwość powiązania na dużą skalę systemów biometrycznych z wykorzystaniem danych biometrycznych w celu ułatwienia krajowych programów identyfikacji tożsamości na dużą skalę. Mimo że pracodawcy mogą zaprojektować system biometryczny wyłącznie do użytku wewnętrznego, aby ułatwić weryfikację tożsamości pracowników w sieciach korporacyjnych, przepisy i prawa federalne, takie jak amerykańska ustawa PATRIOT, mogą ostatecznie zmusić pracodawców do przekazania prywatnych danych biometrycznych pracowników organom rządowym.

Podsumowując, główne obawy dotyczące prywatności związane z wdrożeniami biometrycznymi obejmują:

* Utrata anonimowości i autonomii użytkowników

* Ryzyko nieuprawnionego wykorzystania informacji biometrycznych i / lub nieuprawnionego zbierania informacji biometrycznych

* Niepotrzebne zbieranie informacji biometrycznych

* Nieautoryzowane ujawnianie informacji biometrycznych innym osobom

* Systematyczne ograniczanie rozsądnych oczekiwań użytkowników dotyczących prywatności

* Możliwość nadużycia ze strony nadgorliwych lub skorumpowanych agentów rządowych

Wiele z tych obaw można ogólnie zgrupować pod hasłem „pełzanie funkcji" lub „pełzanie misji", gdzie systemy biometryczne zaprojektowane do uwierzytelniania użytkownika mogą z czasem być wykorzystywane do celów, które nie były pierwotnie zamierzone. Przykładem „pełzania misji" jest stosowanie numerów ubezpieczenia społecznego (SSN) do identyfikacji. Oryginalne karty Ubezpieczenia Społecznego zostały opatrzone stemplem „Nie do identyfikacji". Jednak wiele organizacji (w tym Internal Revenue Service) używa SSN do celów identyfikacji. Niezależnie od zagrożeń dla prywatności, zwolennicy systemów uwierzytelniania biometrycznego argumentują, że systemy biometryczne, odpowiednio wdrożone i z odpowiednią kontrolą najlepszych praktyk, faktycznie mogą funkcjonować w celu wzmocnienia i ochrony prywatności. Woodward, Orlans i Higgins zwracają uwagę, że „kilka nowo opracowanych technologii biometrycznych wykorzystuje cechy fizyczne osoby do skonstruowania kodu cyfrowego dla tej osoby bez zapisywania faktycznych cech fizycznych", tworząc w ten sposób rodzaj szyfrowania biometrycznego, które można wykorzystać do ochrony prywatność danych finansowych, medycznych lub innych osób. Nanavati, Thieme i Nanavati twierdzą, że można zaprojektować systemy biometryczne „współczujące prywatność". Takie systemy:

* Mają ograniczony zakres systemu.

* Unikaj używania danych biometrycznych jako unikalnego identyfikatora.

* Ogranicz przechowywanie informacji biometrycznych.

* Ogranicz przechowywanie możliwych do zidentyfikowania danych biometrycznych.

* Ogranicz gromadzenie i przechowywanie nieistotnych informacji, uwzględniając jednocześnie klauzule „opt-out" dla użytkowników.

* Włącz anonimową rejestrację i weryfikację.

* Zapewnij środki do poprawiania i uzyskiwania dostępu do informacji biometrycznych.

* Ogranicz dostęp do systemu.

* Używaj narzędzi bezpieczeństwa i zasad dostępu, aby chronić informacje biometryczne.

* Przygotuj przepisy dotyczące audytów zewnętrznych.

* Ujawnij cel i cel systemu.

* Ujawnij procesy rejestracji, weryfikacji i identyfikacji.

* Ujawnij obowiązujące zasady i zabezpieczenia, aby zapewnić prywatność informacji biometrycznych.

* Ujawnij postanowienia dotyczące zakończenia systemu

W przeciwieństwie do tego poglądu Alterman twierdzi, że wdrażanie systemów biometrycznych i wykorzystywanie danych biometrycznych do identyfikacji i weryfikacji jest wątpliwe etycznie, ponieważ zawsze wiąże się z naruszeniem prywatności i autonomii. Alterman zauważa „coś niepokojącego w powszechnym stosowaniu identyfikacji biometrycznej poza standardową kwestią prywatności danych". Utrzymuje, że dane biometryczne „mają nieodłączną wartość moralną", ale nie posuwa się nawet do argumentowania przeciwko jakimkolwiek wdrożeniom biometrycznych

systemów identyfikacji lub weryfikacji. Utrzymuje raczej, że należy je rozsądnie wdrażać i wdrażać tylko z należytym uwzględnieniem obaw użytkowników dotyczących prywatności

Kwestie prawne.

W ramach systemu prawnego, jak wspomniano, pojawia się pytanie o zasadność stosowania biometrii. Ponieważ wielu uważa to za naruszenie prywatności na wielu poziomach, należy pokrótce omówić faktyczną definicję tego zjawiska. Zgodnie z obowiązującym prawem istnieją cztery oddzielne kategorie „naruszenia prywatności":

1. Wtargnięcie do twojego życia prywatnego - zwykle jest to robione przez kogoś, kto próbuje potajemnie dowiedzieć się czegoś o tobie.

2. Publiczne ujawnienie prywatnych faktów o sobie przez kogoś innego niż ty sam.

3. Wykorzystanie Twojego imienia i nazwiska, podobizny lub obu tych rzeczy w celu uzyskania korzyści pieniężnych bez Twojej zgody.

4. Każda publikacja stawiająca Cię w fałszywym świetle.

W przypadku biometrii główne obawy wydają się wynikać z pierwszej, a czasem drugiej kategorii. Prawdopodobnie te obawy (i uzasadnione obawy w świetle ostatnich mandatów i działań rządu) można złagodzić poprzez przechowywanie jedynie szablonu cyfrowego lub markera podobnego do tych używanych w algorytmach, a nie faktycznego obrazu. TSA została zmuszona do korzystania ze skanów, które pokazują jedynie podobieństwo osoby w skanerze, a nie rzeczywiste nagie zdjęcie. Firma, z której korzystali do tej pory, nie mogła dostosować się do ich oprogramowania, a tym samym straciła kontrakt. Dzięki temu możliwość trzymania rządu na smyczy i nienaruszania naszych praw konstytucyjnych staje się nieco jaśniejsza.

OSTATNIE TENDENCJE W UWIERZYTELNIANIU BIOMETRYCZNYM

Postępy rządu w dziedzinie uwierzytelniania biometrycznego.

Chociaż organizacje z sektora prywatnego coraz częściej dostosowują technologie biometryczne do potrzeb uwierzytelniania, sektor rządowy (publiczny) jest liderem inwestycji w biometrię. Ataki terrorystyczne z 2001 r. Na World Trade Center i Pentagon oraz późniejsze USA PATRIOT Act zachęcały do zwiększania zaangażowania rządu w technologie biometryczne. Departament Obrony (DoD), Departament Bezpieczeństwa Wewnętrznego (DHS), Służba Imigracji i Naturalizacji oraz Departament Transportu to agencje rządowe najbardziej zaangażowane we wdrażanie technologii biometrycznych. Program Common Access Card Departamentu Obrony obejmuje umieszczenie technologii biometrycznej na inteligentnej karcie identyfikacyjnej.45 Program US-VISIT w ramach DHS to kolejny program rządowy, który włącza dane biometryczne (w tym twarz i odcisk palca) do inteligentnej karty identyfikacyjnej. Inny program DHS, Poświadczenie Tożsamości Pracownika Transportu, zawiera dane biometryczne na karcie identyfikacyjnej.

Skanowanie twarzy na lotniskach iw kasynach.

Po atakach terrorystycznych na World Trade Center i Pentagon w 2001 roku większość krajowych lotnisk przeniosła się na włączenie technologii skanowania twarzy do swoich systemów bezpieczeństwa. Większość badań skuteczności tych systemów ujawniła jednak wysoki poziom błędów i niski poziom dokładności. Kasyna wykorzystują systemy skanowania twarzy do identyfikacji profesjonalnych „graczy korzystających z przewagi" i oszustów. Chociaż jest to w większości nieuregulowane w Stanach Zjednoczonych, kanadyjskie kasyna muszą powiadamiać graczy o

korzystaniu z takich systemów. Kasyna udostępniają dane o profesjonalistach i oszustach. Jedna firma połączyła w sieć 125 operatorów monitorujących kasyna w Stanach Zjednoczonych, Kanadzie, Portoryko, Arubie i na Bahamach i zapewnia alerty w czasie rzeczywistym oraz inne informacje przydatne w identyfikowaniu podejrzanych graczy. Nie jest jednak jasne, jak na takie systemy może wpływać prawo międzynarodowe. Artykuł 12 Powszechnej Deklaracji Praw Człowieka Narodów Zjednoczonych gwarantuje, że „[nikt] nie będzie podlegał arbitralnej ingerencji w swoją prywatność, rodzinę, dom lub korespondencję, ani też atakom na jego honor i dobre imię. Każdy ma prawo do ochrony prawa przed taką ingerencją lub atakami ”46. Sądy nie zajęły się kwestią tego, czy system ten stanowi arbitralną ingerencję lub zamach na czyjeś honor, ale wyraźnie można by postawić sprawę, która potajemnie wykorzystuje takie systemy to robią. Najlepszą praktyką dla każdego systemu nadzoru jest świadoma zgoda. Organizacje powinny wyraźnie publikować powiadomienia o korzystaniu z systemów nadzoru w celu ochrony przed wyzwaniami prawnymi.

Zwiększone rozmieszczenie w branży finansowej.

Branża finansowa, która zwykle powoli wdraża nowe technologie, jest jednym z liderów we wdrażaniu kontroli uwierzytelniania biometrycznego. Obecne wdrożenia obejmują skanery linii papilarnych zabezpieczające sieci komputerowe dla brokerów, systemy rozpoznawania twarzy w bankomatach, a także skanowanie tęczówki oka w punktach dostępu o wysokim poziomie bezpieczeństwa. International Biometric Group przewidywała, że amerykańskie firmy świadczące usługi finansowe wydadzą w 2007 roku 672 miliony dolarów na różne wdrożenia biometryczne. Jednym z największych dotychczasowych wdrożeń było przyjęcie przez United Bankers ’Bancorporation (UBB) U.are.U, systemu rozpoznawania odcisków palców, który umożliwia klientom UBB automatyczne logowanie na stronie internetowej UBB za pomocą skanów palców zamiast haseł. UBB przyjął również system uwierzytelniania odcisków palców dla swoich pracowników. Wells Fargo, Bloomberg Financial i Janus Capital Management to inne znane firmy finansowe, które przyjęły systemy uwierzytelniania biometrycznego dla pracowników i / lub klientów. Chociaż niektóre instytucje finansowe wybrały systemy oparte na głosie, tęczówce lub skanie twarzy, wydaje się, że większość wybiera systemy oparte na skanowaniu odcisków palców.

Biometria w branży opieki zdrowotnej.

Częściowo pobudzone nowymi przepisami, które nakładają na instytucje opieki zdrowotnej obowiązek zapewnienia prywatności i bezpieczeństwa dokumentacji pacjentów, firmy z branży opieki zdrowotnej również przodowały we wdrażaniu uwierzytelniania biometrycznego. Wśród głównych organizacji opieki zdrowotnej, które przeszły na uwierzytelnianie biometryczne, jest Klinika Mayo, która przyjęła system identyfikacji odcisków palców w 2002 r. Większość placówek opieki zdrowotnej, które wdrożyły systemy uwierzytelniania biometrycznego, wybrała systemy identyfikacji oparte na skanach palców. Jednak wdrażanie tych systemów w organizacjach opieki zdrowotnej nie przyniosło takiego samego sukcesu, jak w branży usług finansowych. Kwestie związane z potencjalnym przeniesieniem choroby poprzez fizyczny kontakt ze skanerem linii papilarnych nie są trywialne. Ponadto wskaźniki błędów były wyższe, a wskaźniki dokładności znacznie niższe niż oczekiwano. Wydaje się, że głównym powodem wysokiej częstości błędów są szczegóły dotyczące środowiska opieki zdrowotnej, zwłaszcza cechy rąk lekarzy, pielęgniarek i innych pracowników służby zdrowia korzystających z tych systemów. W szczególności wydaje się, że działanie systemu jest osłabiane przez chronicznie suche ręce tych pracowników, stan wynikający z częstego mycia rąk i stosowania środków odkażających na bazie alkoholu. Innym problemem był opór przed użyciem technologii odcisków palców zarówno przez pielęgniarki, jak i lekarzy, którzy uważają, że wiąże się to z naruszeniem prywatności. Dodajmy do tego koszty, które są związane z powiązaniem typu uwierzytelniania pojedynczego logowania z podstawowym systemem szpitalnym, a problemy nasilą się jeszcze bardziej. Wydaje się, że Cerner i

EPIC mają najlepsze programy w branży opieki zdrowotnej i oba uzyskały certyfikaty dla wszystkich trzech poziomów znaczącego użytkowania wymaganych przez HIPAA i HITECH. Jednak programy te wiążą się z dużymi kosztami. Nawet zwykłe obudowy, ostatnia zmiana na szpital w Wyoming kosztowała ich 4,5 miliona dolarów. Chociaż była to zmiana, którą należało dokonać, rozciągnęła ich budżety do maksimum i dokonano kilku cięć, aby to dostosować.

Zwiększone wdrażanie systemów rejestracji czasu pracy i obecności.

Coraz więcej firm z wielu różnych branż wdraża biometryczne systemy rejestracji czasu pracy. Odchylenie od dotychczasowej praktyki polega na zwiększonym wykorzystaniu biometrycznych systemów obecności i śledzenia pracowników umysłowych. Wcześniej koncentrowano się na robotnikach fabrycznych. Chociaż niektórzy pracodawcy używają tradycyjnych systemów skanowania rąk, wydaje się, że nastąpiła zmiana w kierunku korzystania z systemów rejestracji czasu pracy i obecności przy skanowaniu odcisków palców. Ta zmiana wydaje się być związana z bardziej konkurencyjną strukturą cenową dla systemów czytników linii papilarnych.

PODSUMOWANIE I ZALECENIA.

Nie ma uniwersalnego „najlepszego" systemu uwierzytelniania biometrycznego. Każda z pięciu wiodących technologii biometrycznych ma określone zalety i wady. Niektóre technologie biometryczne są bardziej odpowiednie dla określonych zastosowań i środowisk niż ich odpowiedniki. Organizacja w trakcie oceny potencjalnej implementacji uwierzytelniania biometrycznego musi zdawać sobie sprawę z tego, że przy każdym wyborze pojawią się kompromisy, takie jak koszt dokładności, prywatność w porównaniu z akceptacją przez użytkownika itd. konkretna technologia biometryczna do określonego zastosowania. Istnieje jednak wiele badań dotyczących wielu zalet i wad biometrii. Rysunek 29.3 zawiera podsumowanie porównania cech pięciu wiodących technologii biometrycznych omówionych w tym rozdziale. Cechy, pokazane w skrajnej lewej kolumnie, pochodzą z różnych prac badawczych, a rankingi stanowią połączenie rankingów znalezionych w literaturze. Chociaż systemy uwierzytelniania biometrycznego obiecują oszczędności kosztów i wyższy poziom bezpieczeństwa dla organizacji, nie stanowią panaceum. Wiele czynników wpływa na to, jak dobrze lub słabo sprawdzą się mechanizmy uwierzytelniania biometrycznego w danym środowisku organizacyjnym. Wśród tych czynników znajdują się użytkownicy, administracja, środowisko, infrastruktura, budżet, system komunikacji i istniejące potrzeby w zakresie bezpieczeństwa. Chociaż wiele technologii biometrycznych może działać jako samodzielne systemy, w rzeczywistości ich dokładność i poziom wydajności uległyby znacznej poprawie poprzez połączenie ich z bardziej konwencjonalnymi metodami uwierzytelniania, takimi jak hasła i klucze. Takie systemy wieloczynnikowe zapewniają większe bezpieczeństwo i niezawodność. Wybierając biometryczny system uwierzytelniania i przygotowując się do wdrożenia, organizacje powinny skupić się na interfejsie technologii użytkownika i warunkach w środowisku operacyjnym, które mogą mieć wpływ na wydajność technologii. Na przykład bezrefleksyjne przyjęcie technologii skanowania odcisków palców w branży opieki zdrowotnej ilustruje niebezpieczeństwa wynikające z nieuwzględnienia realiów środowiskowych. Ważne jest, aby organizacje brały pod uwagę nie tylko praktyczne przeszkody w skutecznym wdrażaniu, ale także potencjalne przeszkody psychologiczne, takie jak obawy użytkowników dotyczące technologii. Z etycznego punktu widzenia organizacja ma również obowiązek uważnego rozważenia zakresu, w jakim wdrożenie uwierzytelniania biometrycznego narusza prawa użytkowników do prywatności. Dokonując tej oceny, kierownictwo musi wziąć pod uwagę możliwość, że organizacja może zostać zmuszona do udostępnienia organom rządowym informacji biometrycznych pracowników. Ostatnie badania biometryczne obejmują banki i inne instytucje finansowe, które wskazały wykorzystanie biometrii głosowej zamiast identyfikacji odcisków palców jako jeden z najlepszych sposobów zabezpieczenia rachunków klientów i informacji finansowych. Biometria głosu porównuje różne cechy zaczerpnięte z głosu klienta, takie jak fleksja,

tonacja, dialekt, akcent i inne, dopasowując je do wcześniej zarejestrowanych i bezpiecznie przechowywanych danych. Aby ta technologia działała, będzie jednak wymagać od banków i innych instytucji finansowych zarejestrowania wzorców głosu klientów, skorelowania ich z danymi osobowymi i umieszczenia ich w bazie danych. Inne badania doprowadziły do zawarcia umów z dużymi korporacjami, aby pomóc w branży opieki zdrowotnej, np. BIO-Key zawarł umowę OEM z Caradigm na korzystanie z pakietu BIO-Key do zarządzania tożsamością i dostępem. Caradigm zaoferuje ten pakiet w ramach swojego rozwiązania Single Sign On, aby pomóc szpitalom i innym opiekunom w pisaniu elektronicznych recept na substancje kontrolowane w spełnieniu przepisów federalnych i stanowych48. celów identyfikacyjnych, rozpoznawania żył i platform mobilnych używanych do promowania ich akceptacji. W raporcie z 2011 roku opublikowanym przez Unisys Corporation, akceptacja tych i innych technologii biometrycznych rośnie, ale wolniej niż przewidywano.