Łukasz Stasiak, Adam Czajka, Przemysław Strzelczyk, Marcin Chochowski, Andrzej Pacut, "Od biometrii do bezpiecznej biometrii", *SECURE 2006 Bezpieczeństwo - czas na przełom*, Warszawa, 17-18 października 2006

OD BIOMETRII DO BEZPIECZNEJ BIOMETRII

Łukasz Stasiak, Adam Czajka, Przemysław Strzelczyk,
Marcin Chochowski, Andrzej Pacut
Pracownia Biometrii, Naukowa i Akademicka Sieć Komputerowa
Instytut Automatyki i Informatyki Stosowanej, Politechnika Warszawska

Wstęp

W ujęciu tradycyjnym “biometria” oznaczała technikę dokonywania pomiarów istot żywych w celu przeprowadzenia ilościowych badań nad zmiennością populacji [1]. Obecnie znaczenie pojęcia zostało rozszerzone i oznacza “zautomatyzowane metody identyfikacji lub weryfikacji tożsamości żyjącej osoby na podstawie cech fizjologicznych lub behawioralnych” [2]. W jednym, jak i w drugim znaczeniu biometria szeroko korzysta z metod statystyki matematycznej.

“Zautomatyzowane metody identyfikacji lub weryfikacji” oznaczają pełną automatyzację całego procesu od momentu pobrania odpowiedniej charakterystyki, poprzez obróbkę i analizę aż do udzielenia przez system odpowiedzi dotyczącej rozpoznawanej tożsamości. Mimo iż większość współczesnych systemów biometrycznych wymaga pewnego minimalnego stopnia współpracy ze strony użytkowników na etapie pomiaru charakterystyki, to już sam proces przetwarzania pobranych danych jest w zupełności autonomiczny i nie wymaga, poza administracyjnym ustawieniem pożądanego poziomu “restrykcyjności” systemu, dodatkowej interwencji ze strony użytkowników. Dane biometryczne są na stałe “związane” z osobą, co zwiększa wygodę ich użycia (nie trzeba nic pamiętać, np. hasła, ani też nosić ze sobą dodatkowych przedmiotów, np. kluczy), a tym samym przyczynia się do szerszej akceptacji takich rozwiązań przez użytkowników. Z punktu widzenia administratora zabezpieczeń dane biometryczne pozwalają na bezpośrednie, teoretycznie nierozerwalne, połączenie procesu uwierzytelniania z osobą, a nie z hasłem czy tokenem. Osobnicze charakterystyki biometryczne są trudne do sfałszowania, a ich zmiana zwykle wymaga trudnych zabiegów chirurgicznych. Z tego powodu próby złamania zabezpieczeń biometrycznych rzadko polegają na zamianie oryginalnych charakterystyk biometrycznych osoby, lecz zwykle wykorzystują luki w samym procesie przetwarzania, przesyłania i przechowywania danych. Takie luki występują najczęściej na styku (interfejsie) poszczególnych bloków składowych całego procesu, w szczególności na styku człowiek – urządzenie pomiarowe, urządzenie pomiarowe – system przetwarzania oraz system przetwarzania – baza danych biometrycznych.

Wydarzenia z 11 września 2001 spowodowały gwałtowny wzrost zainteresowania metodami biometrycznymi. Producenci i dostawcy rozwiązań biometrycznych rozpoczęli bitwę o rynek, prezentując coraz to doskonalsze urządzenia i systemy. W wyniku takiego wzrostu zainteresowania, często naprędce wprowadzane na rynek rozwiązania nie cechowały się dostateczną jakością, a walka o klienta sprowadzała się jedynie do doskonalszych chwytów marketingowych. Jednocześnie gotowe elementy systemów biometrycznych,

często niedoskonałe, trafiały w ręce niewykwalifikowanych integratorów, którzy zapominali o konieczności stosowania do systemów biometrycznych ogólnych zasad obowiązujących przy tworzeniu dowolnych systemów zabezpieczeń. Tym bardziej nie stosowano specyficznej wiedzy wymaganej przy implementacji metod biometrycznych. Niedoskonałości urządzeń biometrycznych w połączeniu z ich niefachowym wykorzystaniem sprawiły, że wiele osób zaczęło postrzegać biometrię jedynie jako przejściową modę, a nie faktyczny przełom w systemach zabezpieczeń. Do tego dołączyły głosy sprzeciwu wieszczące, iż biometria to kradzież tożsamości i prowadzi do ograniczenia wolności w stylu orwellowskiego roku 1984. Oczywiście faktem jest, że wiele z popełnionych błędów wynikało również z “okresu niemowlęctwa”, w jakim znajdowała się biometria. Tym bardziej pochopne stosowanie metod biometrycznych mogło przynosić niezadowalające i niespodziewane skutki.

W chwili obecnej zarówno rozwój urządzeń pomiarowych, jak i wiedza o architekturze systemów biometrycznych (często zapożyczona z innych, starszych dziedzin informatyki, szczególnie kryptografii i telekomunikacji) pozwalają na tworzenie pewnych systemów bezpieczeństwa wykorzystujących elementy biometryczne. Właśnie spojrzenie na rozwiązania biometryczne jako element szerszej infrastruktury bezpieczeństwa, a nie jako system sam w sobie, jest kluczem do sukcesu. Kluczem, który pozwoli zastosować biometrię w sposób zwiększający bezpieczeństwo całego systemu przy jednoczesnym zwiększeniu wygody użytkowników.

W kolejnych rozdziałach prześledzimy drogę danych biometrycznych w systemie bezpieczeństwa. Zwrócimy uwagę na zagrożenia związane z poszczególnymi etapami oraz pokażemy w jaki sposób te zagrożenia minimalizować.

1. Budowa systemu biometrycznego

System biometryczny może zostać podzielony na kilka podstawowych bloków odpowiedzialnych za realizację różnych funkcji systemu. Zestaw takich bloków, a szczególnie ich wewnętrzna realizacja mogą też różnić się w zależności od przeznaczenia całego systemu biometrycznego. Widać to zwłaszcza w przypadku porównania systemów weryfikacji tożsamości z systemami identyfikacji tożsamości. Pierwsze z nich wykonują porównanie pobranych danych biometrycznych z jednym wzorcem, a decyzja zwracana przez system ma charakter binarny (typu “potwierdzam/odrzucam”) – system potwierdza tożsamość użytkownika lub nie może jej potwierdzić. Z kolei systemy identyfikacji wykonują znaczną liczbę porównań pomiędzy danymi pochodzącymi od badanego użytkownika[1], a wieloma (lub nawet wszystkimi) wzorcami biometrycznymi zgromadzonymi w obszernej bazie danych. Decyzja systemu ma zwykle mniej autorytatywny charakter i zwracana jest lista

1 Należy zauważyć, że automatyczna identyfikacja tożsamości może być wykonywana bez zgody czy nawet wiedzy osoby badanej, co rodzi potrzebę prac legislacyjnych w celu wprowadzenia odpowiednich regulacji prawnych w zakresie identyfikacji biometrycznej.

tożsamości najlepiej pasujących do danego użytkownika. Poszczególne pozycje listy mają najczęściej jawnie przypisane wagi.

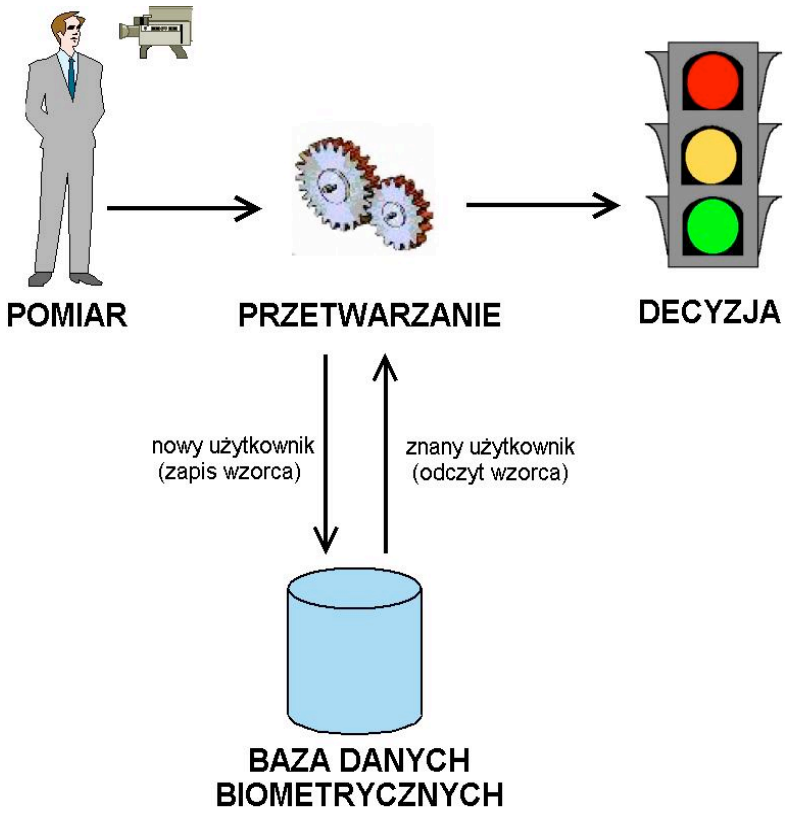
Oczywiście w przypadku podziału systemu na pojedyncze bloki, tak jak ma to miejsce przy każdego rodzaju dekompozycji czy klasyfikacji, pozostaje pytanie o poziom, na którym zostanie ona przeprowadzona. Nie wchodząc zanadto w szczegóły stosowanych technik i przy zachowaniu należytego stopnia adekwatności uproszczonego modelu do większości systemów biometrycznych możemy w nich wyróżnić następujące bloki:

- pomiaru – blok odpowiedzialny za pomiar charakterystyk biometrycznych użytkownika, jednocześnie jest to miejsce bezpośredniego styku użytkownika z systemem; w skład tego bloku wchodzą różnego rodzaju czytniki i czujniki;
- przetwarzania – w tym bloku surowe dane biometryczne zostają przetworzone do odpowiedniej postaci matematycznej, co ma umożliwić ich łatwą klasyfikację i przechowywanie, nie tracąc przy tym informacji indywidualnej związanej z oryginalną charakterystyką biometryczną; również w tym bloku następuje porównanie bieżącej charakterystyki z charakterystykami przechowywanymi w pamięci systemu; w skład tego bloku wchodzą najróżniejsze techniki obróbki sygnałów (w szczególności obrazu) oraz ekstrakcji cech;
- przechowywania – każdy system biometryczny (weryfikacji lub identyfikacji tożsamości) musi dysponować odpowiednim rodzajem pamięci do przechowywania wzorców cech biometrycznych użytkowników systemu, często blok przechowywania odpowiada również za aktualizację wzorców, które mogą być zmienne w czasie; w skład tego bloku wchodzą systemowe bazy danych biometrycznych;
- decyzji – blok decyzji odpowiada za udzielenie przez system oczekiwanej odpowiedzi (np. binarnej typu “potwierdzam/odrzucam” lub w postaci listy odpowiadających tożsamości) w zależności od wyników zwróconych przez blok przetwarzania; blok decyzji może być postrzegany jako element bloku przetwarzania, jednakże jego ideowe wydzielenie pozwala zwrócić uwagę na możliwość administracyjnej konfiguracji systemu, to właśnie w bloku decyzji administrator systemu dostraja wartości odpowiednich parametrów zmieniając poziom “restrykcyjności” całego systemu, często jest to jedyne “otwarte” miejsce w systemie, umożliwiające zmianę jego własności bez konieczności naruszenia jego zamkniętej struktury.

Z punktu widzenia użytkownika systemy biometryczne wykorzystujące różne typy charakterystyk różnią się przede wszystkim sposobem ich pomiaru, a więc wyglądem urządzenia pomiarowego. Tymi urządzeniami mogą być kamery (biometria tęczówki, twarzy), skanery (biometria dłoni, odcisków palców), czujniki naciskowe i ultradźwiękowe (biometria odcisków palców, linii papilarnych wnętrza dłoni), tablety graficzne (biometria podpisu odręcznego), mikrofony (biometria głosu) czy nawet czujniki zapachu lub klawiatura komputera (biometria dynamiki pisania na klawiaturze). Z punktu widzenia konstruktorskiego każda charakterystyka biometryczna wymaga specyficznego podejścia na etapie pomiaru i przetwarzania. Metody dotyczące

przechowywania są bardziej ogólne i mogą być stosowane do wszystkich rodzajów biometrii, choć często pojawiają się specyficzne ograniczenia (np. wielkość wzorca) wymuszające zastosowanie nietypowych rozwiązań dla poszczególnych technik biometrycznych.

Schemat systemu biometrycznego z wydzielonymi głównymi blokami przedstawiono na rys. 1. Pomiar w systemie przedstawionym na schemacie odbywa się za pomocą kamery, a ze względu na charakter decyzji wyjściowej system może być postrzegany jako system weryfikacji tożsamości.



Rysunek 1: Schemat typowego systemu biometrycznej weryfikacji.

Każdy z bloków systemu biometrycznego narażony jest na inne nadużycia, każdy więc musi być inaczej chroniony. Należy również zwrócić uwagę, iż kanały komunikacyjne pomiędzy poszczególnymi blokami stanowią część systemu, a więc muszą być również odpowiednio zabezpieczone. Warto jednak zauważyć, że przedstawione na rys. 1 bloki logiczne nie zawsze oznaczają oddzielne bloki fizyczne. W takiej sytuacji zabezpieczenie kanałów komunikacyjnych przebiegających wewnątrz jednego urządzenia fizycznego jest łatwiejsze i może być sprowadzone do odpowiedniego zabezpieczenia urządzenia jako całości.

Próby złamania systemu biometrycznego mogą koncentrować się na różnych blokach tego systemu. Wiele rodzajów możliwych ataków nie różni się w swojej specyfice od ataków mogących dotyczyć dowolnych systemów informatycznych. I tak np. próby ataku na etapie przetwarzania danych

oznaczają zamianę głównych algorytmów systemu. Może to być dokonane poprzez bezpośrednią ingerencję w sprzęt, bądź też w oprogramowanie. Ważne pozostają tu więc zasady ochrony fizycznej oraz przeciwwłamaniowej i przeciwwirusowej znane z innych działów budowy systemów informatycznych. Dla wszystkich zresztą elementów biometrycznego systemu bezpieczeństwa należy stosować dobre praktyki obowiązujące przy konstruowaniu dowolnych, bezpiecznych systemów informatycznych [3]. W tym miejscu warto również podkreślić, iż tak jak w przypadku innych systemów zabezpieczeń, użytkownik systemu jest jego ważną częścią. Aby część ta nie była najsłabszym ogniwem, użytkownik musi zawsze zostać odpowiednio przeszkolony w zakresie korzystania z danego systemu i możliwych nadużyć.

Arsenał zagrożeń dotyczących systemów biometrycznych, ze względu na ich specyfikę, jest jednak nieco szerszy niż w przypadku “zwykłych” systemów informatycznych. Celem niniejszego artykułu jest przedstawienie tego typu swoistych zagrożeń i sposobów przeciwdziałania im. W przypadku systemów biometrycznych zagrożenia te dotyczą przede wszystkim:

- pomiaru charakterystyk biometrycznych,
- przesyłania danych biometrycznych,
- przechowywania danych biometrycznych.

W kolejnych rozdziałach szczegółowo przedstawimy kolejne zagrożenia. Prezentowane poniżej metody będą dotyczyły wykorzystania biometrii tęczówki. Są to metody opracowane w Pracowni Biometrii NASK i zaimplementowane w prototypowym urządzeniu biometrii tęczówki NASK IRS (ang. *Iris Recognition System*). Dla lepszego zrozumienia zagadnienia, zanim przedstawimy specyfikę poszczególnych zagrożeń, w kolejnym rozdziale pokrótce scharakteryzujemy budowę i działanie systemu tęczówki NASK IRS.

2. System rozpoznawania tęczówki – krótka charakterystyka

Idealna cecha biometryczna, służąca do rozpoznawania osób (weryfikacji lub/i identyfikacji tożsamości) powinna spełniać kilka kryteriów. Najważniejsze z nich to:

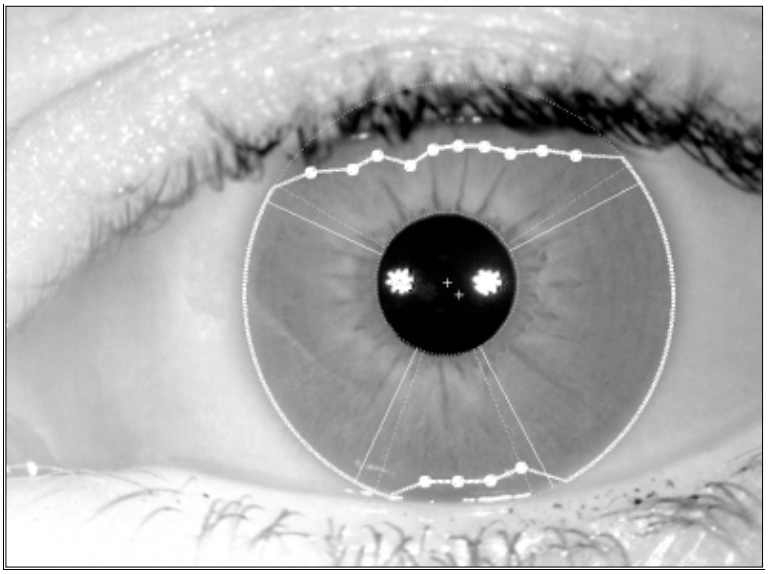
- uniwersalność – każdy człowiek ją ma,
- unikalność – każdy ma ją inną,
- niezmienność – cecha nie zmienia się w ciągu życia,
- mierzalność – można dokonać pomiarów ilościowych cechy,
- akceptowalność – wykonywanie pomiaru danej cechy nie powinno budzić wśród użytkowników zastrzeżeń natury zdrowotnej, społecznej czy religijnej.

W przypadkach praktycznych, żadne z powyższych wymagań nie może być całkowicie spełnione, stąd wymagania są rozluźniane i tak np. “uniwersalność” rozumie się jako wymóg, iż pewna “znaczna większość” grupy użytkowników docelowych posiada daną cechę (dla pozostałych stosuje się rozwiązania alternatywne), a “niezmienność” w czasie staje się jedynie “wolną zmiennością” (tak, aby system potrafił nauczyć się tych zmian). Okazuje się także, iż spełnienie wymogu pełnej akceptowalności może być w pewnych sytuacjach trudne do zrealizowania. Jedną z przyczyn tej trudności może być narastające we współczesnym świecie wymieszanie kulturowe i etniczne (np. w pewnych

kulturach fotografowanie twarzy kobiet jest zakazane). Oprócz powyższych wymagań związanych z biologiczną naturą cechy, pojawiają się też inne wymagania natury inżynierskiej, zależne od konkretnego rozwiązania, takie na przykład jak czas przetwarzania, łatwość pomiaru, maksymalna liczba użytkowników systemu itp.

Tęczówka okazuje się być jedną z tych cech biometrycznych, które najlepiej spełniają wszystkie postawione wymagania. Jest ona nie tylko źródłem cech o wysokim stopniu zróżnicowania dla populacji ludzkiej (unikalność), ale dodatkowo bardzo stabilnych w czasie (niezmienność). Współczesne systemy biometrii tęczówki są szybkie i odznaczają się wysoką dokładnością weryfikacji. W miarę rozwoju metod optycznych, pomiar staje się dla użytkownika coraz mniej uciążliwy.

Pełny proces weryfikacji lub identyfikacji z wykorzystaniem tęczówki odpowiada ogólnemu schematowi przedstawionemu na rys. 1. Rejestracja obrazu tęczówki odbywa się w trybie interaktywnym i trwa średnio 5 sekund. Czas przetwarzania obrazu, wraz z lokalizacją tęczówki, wyznaczeniem cech i porównaniem wzorców trwa około 3,5 sekundy. Obraz tęczówki uzyskany z wykorzystaniem systemu NASK IRS, wraz ze zlokalizowaną tęczówką, zakłóceniami i automatycznie wybranymi sektorami podlegającymi kodowaniu przedstawia rys. 2. Analiza wyodrębnionej z obrazu tęczówki może być przeprowadzona z wykorzystaniem wielu różnych metod. System NASK IRS wykorzystuje nową metodę kodowania cech tęczówki, bazującą na rozwinięciu Zaka-Gabora wzbogaconą o algorytmy doboru współczynników rozwinięcia w zależności od jakości przetwarzanych zdjęć tęczówki oraz technikę dynamicznej zmiany wzorca biometrycznego w celu ich ochrony przed niepowołanym użyciem. Więcej szczegółów odnośnie technik przetwarzania, analizy i kodowania tęczówki Czytelnik znajdzie w [4,5].



Rysunek 2: Obraz oka ze zlokalizowaną tęczówką i automatycznie dobranymi sektorami bez zakłóceń.

W kolejnych rozdziałach przedstawimy najważniejsze zagrożenia dla bezpieczeństwa systemu dotyczące pomiaru, przesyłania i przechowywania danych biometrycznych. Jak zaznaczono wcześniej, prezentowane przykłady będą dotyczyć systemu biometrii tęczówki NASK IRS.

3. Pomiar charakterystyk biometrycznych

Pomiar charakterystyk biometrycznych, ze swej natury nierozerwalnie związanych z użytkownikiem, to moment, w którym zostają one przekształcone do postaci pewnych danych biometrycznych (które mogą być dalej przetwarzane i przekształcane) i w tej formie wprowadzone do systemu. W systemie dane te mogą pozostać jedynie na czas analizy, po czym zostaną usunięte. Mogą też być przechowywane w trwałej pamięci systemu.

Niezależnie od dalszych działań związanych z danymi biometrycznymi, bezpieczeństwo systemu może zostać zagrożone już na etapie pomiaru charakterystyk biometrycznych. Bezpieczeństwo systemu na tym etapie przetwarzania wiąże się ze stwierdzeniem autentyczności podsystemu pomiarowego (dotyczy szczególnie pomiaru zdalnego) oraz autentyczności próbki biometrycznej. Pierwszy rodzaj zagrożeń jest równoważny problemowi uwierzytelniania urządzeń w sieci i może być rozwiązany za pomocą znanych metod bazujących na “wspólnym sekrecie” lub wzajemnej walidacji certyfikatów [6,7]. Drugi rodzaj zagrożeń jest typowy dla systemów biometrycznych i oznacza konieczność automatycznego stwierdzenia czy próbka jest autentyczna i reprezentuje żywy obiekt. Idealny system mógłby również analizować stan emocjonalny użytkownika, aby wykluczyć, iż działa on pod przymusem. Taka analiza jest ciągle jeszcze niemożliwa, jakkolwiek prowadzone są badania dotyczące reakcji oka w sytuacjach stresowych oraz

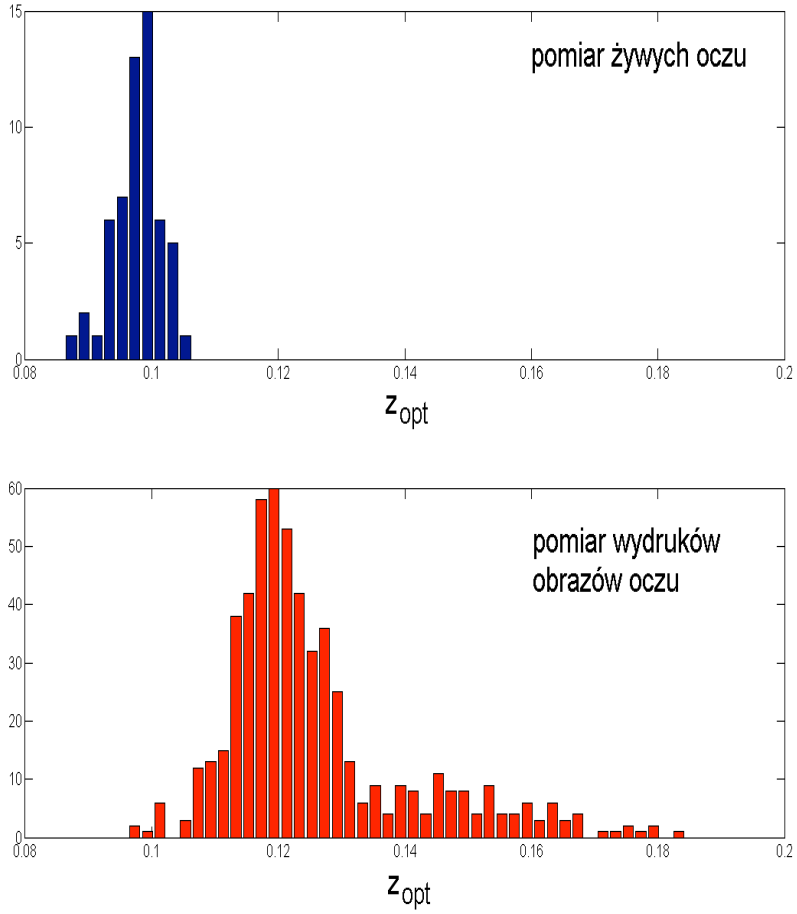
nad zastosowaniem nowych metod biometrycznych, które umożliwiałyby badanie stanów emocjonalnych (np. biometria fal mózgowych EEG [14]). Automatyczny proces stwierdzenia autentyczności próbki dla biometrii bazujących na pomiarze cech fizycznych określa się mianem “testu żywotności” (ang. *aliveness detection*).

Próby oszukania systemu biometrycznego (podszycia się pod innego użytkownika) na etapie pomiaru polegają najczęściej na próbie użycia sztucznie wygenerowanej cechy biometrycznej zamiast cechy autentycznej. Jakość sztucznych cech może być niska (np. prosty wydruk obrazu oka) lub wysoka (np. sztuczna gałka oczna), co wiąże się z różnym kosztem przygotowania takich falsyfikatów. Niestety współcześnie wiele systemów biometrycznych nie zawiera nawet mechanizmów przeciwdziałania najprostszym fałszerstwom. Badania przeprowadzone przez niemiecki Instytut Fraunhofera we współpracy z niemieckim Urzędem ds. Bezpieczeństwa Technik Informacyjnych (BSI) [8] oraz niezależnie przez Pracownię Biometrii NASK [15] wykazały, że nawet szeroko stosowane w praktyce biometryczne systemy zabezpieczeń nie posiadają odpowiednich mechanizmów chroniących przed tego typu nadużyciami. W szczególności pokazano, iż popularne systemy biometrii tęczówki udaje się oszukać z wykorzystaniem wydruków oka przygotowanych przy użyciu zwykłej drukarki laserowej.

Techniki “oszukiwania” systemu biometrii tęczówki możemy podzielić na kilka grup w zależności od ich zaawansowania, co pozostaje w ścisłym związku z klasyfikacją pod względem zaawansowania technik przeciwdziałania tym fałszerstwom. Pierwsza grupa metod zapobiegania fałszerstwom opiera się na badaniu zewnętrznych cech oka. Druga grupa metod bierze pod uwagę wewnętrzne właściwości oka, a ściślej tkanki, z której zbudowane jest oko. Wreszcie trzecia grupa metod bazuje na dynamicznych właściwościach oka ludzkiego. Metody zaliczane do każdej z powyższych grup mogą mieć charakter pasywny lub aktywny. Przykłady rozwiązań zaproponowanych przez zespół Pracowni Biometrii NASK, zostały opisane w kolejnych podrozdziałach.

3.1 Analiza częstotliwościowa

Analiza częstotliwościowa pozwala na łatwe wykrycie sztucznych regularności występujących na obrazie, które pojawiają się m.in. na obrazach wydrukowanych za pomocą urządzeń rastrowych, czyli np. zwykłej drukarki. Dobór parametrów metody (systemu) odbywa się poprzez optymalną selekcję odpowiedniego zakresu częstotliwości, w ramach którego widmo amplitudowe wykazuje największe różnice dla obrazów żywych oczu i ich wydruków. Dokonuje się tego z wykorzystaniem specjalnie utworzonej bazy wydruków tęczówek, uwzględniając różne rozdzielczości i nośniki wydruków oraz różne maszyny drukujące. Przykładowe rozkłady widma amplitudowego dla obrazów żywych oczu oraz wydruków obrazów oczu przedstawia rys. 3.



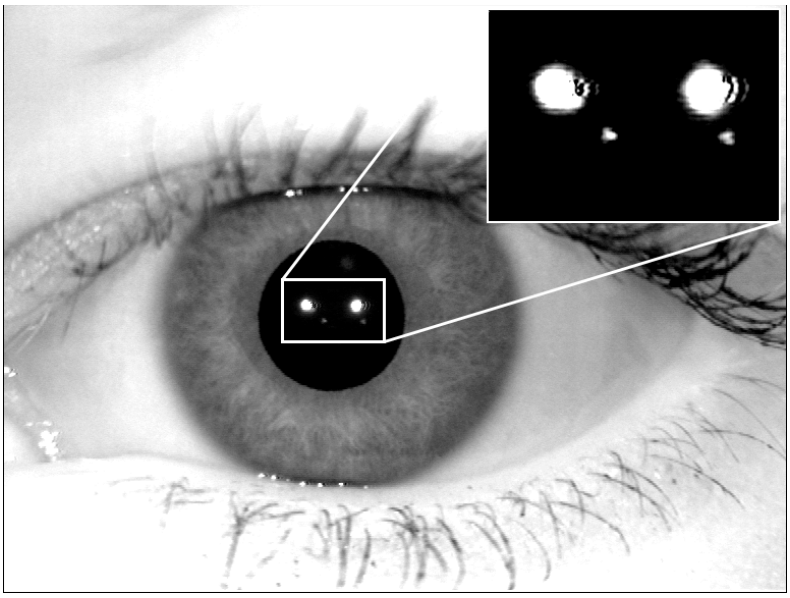
Rysunek 3: Rozkłady zawartości procentowej widma amplitudowego dla obrazów żywych oczu i ich wydruków, wyznaczone dla optymalnych parametrów systemu.

Główną zaletą tej metody jest brak szczególnych wymagań dotyczących stosowanego sprzętu – analiza częstotliwościowa jest przeprowadzana na bazie tego samego obrazu, na którym przeprowadzany jest proces rozpoznawania tęczówki. Ograniczenie metody wynika z teorii Shannona: metoda staje się mniej dokładna, gdy rozdzielczość drukarki użytej do przygotowania wydruku oka jest ponad dwukrotnie większa niż rozdzielczość kamery pomiarowej w systemie biometrycznym. Mimo to, ta prosta metoda skutecznie posłużyła do wykrycia około 95% fałszerstw podczas testów laboratoryjnych.

3.2 Analiza odbić źródła światła.

Pasywna analiza odbicia światła od gałki ocznej może opierać się na wiedzy dotyczącej wewnętrznej budowy gałki ocznej [9,10]. Metody te analizują wygląd oka przy stosowaniu światła o różnej długości fali. Melanina, będąca substancją odpowiedzialną za kolor oka, ma specyficzny profil absorpcji światła. Znajomość tego profilu pozwala na odróżnienie żywej tkanki od imitacji oka wykonanej z tworzyw sztucznych. Z kolei pojawianie się tzw. odbić Purkinjego jest skutkiem warstwowej budowy oka ludzkiego i wynikającego stąd podwójnego odbicia od rogówki i soczewki, które dodatkowo nie są idealnie

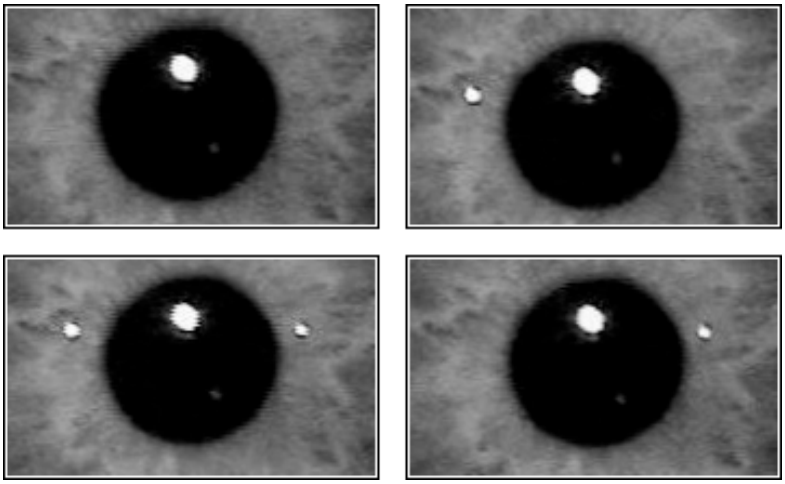
sferyczne. Z drugiej strony odbicia te są stosunkowo trudne do obserwacji i najczęściej jedynie dwa spośród czterech odbić Purkinjego są łatwo obserwowalne, rys. 4.



Rysunek 4: Dwie pary odbić Purkinjego. Zdjęcie uzyskane za pomocą systemu NASK IRS.

Innym podejściem wykorzystującym pomiar aktywny jest analiza odbicia pochodzącego ze sztucznej stymulacji oka światłem podczerwonym. W tym celu urządzenie NASK IRS zostało wyposażone w dwie dodatkowe diody umieszczone po obu stronach obiektywu. Dwie diody umożliwiają realizację czterech różnych stanów oświetlenia (odbicia): każda z dwóch diod może być zapalona lub zgaszona, patrz rys. 5 (odbicie centralne jest wynikiem oświetlenia głównego stosowanego ze względu na proces rozpoznawania, dwie diody sygnałowe są widoczne w postaci małych plamek po prawej i lewej stronie źrenicy, na obszarze tęczówki).

Dodatkowe diody umieszczono tak, aby odbicia były generowane na obszarze tęczówki, a nie źrenicy. Próby fałszerstw z użyciem wydruku wymagają zwykle wycięcia otworu w miejscu źrenicy na wydruku i przyłożenia go do własnego oka: w takim wypadku fałszowany jest wzór tęczówki, podczas gdy źrenica pozostaje “autentyczna”. Odbicia pojawiające się w obszarze tęczówki uniemożliwiają więc zastosowanie takiej prostej metody fałszerstwa. Fałszerz mógłby oczywiście przygotować wydruki obrazu oka wraz z naniesionymi na nie odbiciami. Aby uniemożliwić tego typu fałszerstwo równolegle z rejestracją obrazu tęczówki do celów rozpoznawania generowana jest losowa sekwencja stanów diod oświetlających. Porównanie zarejestrowanej przez system sekwencji odbić z sekwencją wygenerowaną przez system pozwala zaklasyfikować obraz oka jako pochodzący od oka prawdziwego lub falsyfikatu. Zastosowanie losowej sekwencji 8 stanów diod kontrolnych w systemie NASK IRS wydłuża cały proces rozpoznawania tęczówki o ok. 2 sekundy.

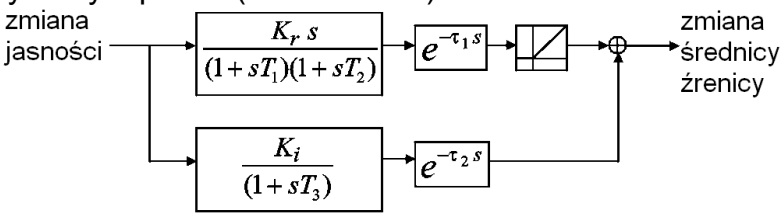


Rysunek 5: Cztery możliwe stany stymulowanych odbić światła od gałki ocznej.

Metoda ta pozwala na wykrycie fałszerstw z użyciem wydruków wysokiej jakości. W połączeniu z proponowaną przez Daugmana analizą profilu absorpcji światła może być także stosowana do wykrywania fałszerstw z użyciem bardziej wyszukanych falsyfikatów, tzn. takich, na których będą występowały odbicia od diod kontrolnych.

3.3 Analiza dynamiki źrenicy

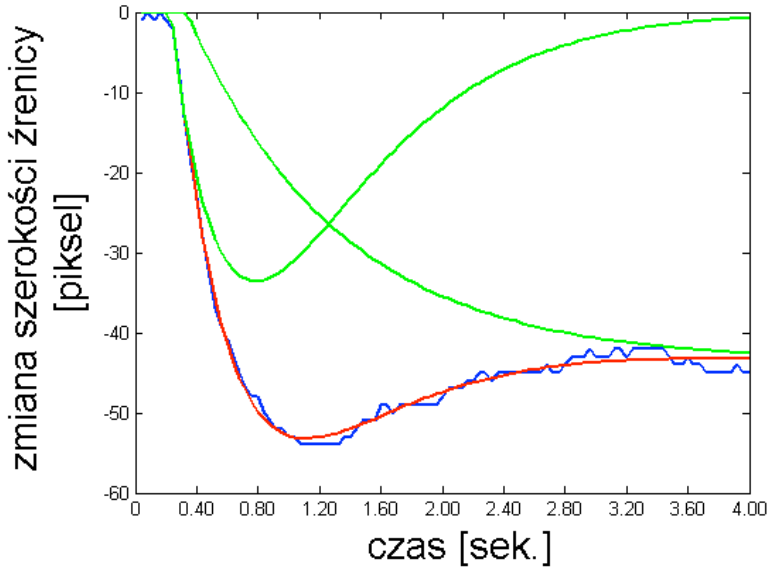
Analiza dynamiki źrenicy pozwala przeciwdziałać atakom z użyciem bardziej zaawansowanych, aktywnych falsyfikatów oka faktycznego użytkownika systemu. Model odpowiedzi źrenicy na skokowy dodatni impuls świetlny został zaproponowany już przez Clynesa i Kohna w 1967 r. [12]. Model składa się z dwóch niezależnych torów, inercyjnego i różniczkującego, rys. 6. Należy pamiętać jednak, że model ten nie wyjaśnia pełnego zjawiska kurczenia się i rozszerzania źrenicy w odpowiedzi na zmianę jasności światła docierającego do oka, a jedynie modeluje sytuację, gdy oko stymulowane jest światłem o wybranym profilu (skok dodatni).



Rysunek 6: Model odpowiedzi źrenicy oka ludzkiego na skokowy dodatni impuls świetlny.

W celu zarejestrowania dynamiki źrenicy każdego z użytkowników zapisywana jest 4 sekundowa sekwencja (25 klatek na sekundę) rejestrowana od momentu zaistnienia bodźca świetlnego. Zarejestrowana sekwencja jest następnie analizowana i przekształcana do postaci ciągu wartości średnicy źrenicy w danych chwilach czasowych. Jako cechy służące odróżnieniu reakcji żywego oka od reakcji falsyfikatu służą parametry modelu zaobserwowanej reakcji, tj. parametry T_1, T_2, T_3, τ_1, τ_2, K_r oraz K_i (rys. 6). Cechy te są wyodrębniane poprzez znalezienie najlepszego dopasowania wyjść modelu do

wartości zaobserwowanego ciągu. Przykładowe dopasowanie modelu do zaobserwowanego ciągu wartości przedstawiono na rys. 7. Klasyfikacja wyodrębnionych wartości cech – jako pochodzących od autentycznej bądź fałszywej próbki – odbywa się z wykorzystaniem klasyfikatorów nieliniowych (np. sieci neuronowej).



Rysunek 7: Przykładowe dopasowanie wyjścia modelu (linia czerwona) do danych eksperymentalnych (linia niebieska). Linie zielone – odpowiedzi poszczególnych torów modelu.

Zastosowanie analizy dynamiki źrenicy pozwala na odrzucenie wszelkich prób fałszerstwa z użyciem falsyfikatów statycznych, nawet bardzo dobrej jakości i przechodzących prostsze testy żywotności opisane powyżej (w drastycznym przypadku z użyciem martwej, ale autentycznej gałki ocznej). Nawet w przypadku wykorzystania bardziej zaawansowanych, ruchomych imitacji fałszerz jest zmuszony podjąć dodatkowy trud związany z koniecznością dopasowania reakcji falsyfikatu do reakcji oka ludzkiego, a także z pomiarem impulsu świetlnego wyzwalającego początek reakcji.

3.4 Podsumowanie

Jak widać metody testowania żywotności, podobnie jak i fałszerstwa, mogą być proste, jak i bardziej wyszukane. Ich dobór zależy od wymagań stawianych danemu systemowi. Niestety użycie każdej z tych metod wydłuża nieco czas przetwarzania – w przypadku prostszych metod dodatkowy narzut jest jednak bardzo niewielki. W złożonym systemie, wyposażonym w pełny zakres testów żywotności możliwe jest zastosowanie testów kaskadowych – od najprostszych do najbardziej skomplikowanych: odrzucenie na dowolnym etapie oznacza przerwanie całego procesu. Poza samym etapem rejestracji tęczówki użytkownika możliwe jest również zrównoleglenie procesu przetwarzania: jedne procesory mogą przetwarzać obraz w kierunku identyfikacji i/lub weryfikacji tożsamości, a inne w kierunku testu żywotności. Inwestycja w rozbudowę systemu o testy żywotności jest jednak korzystna, gdyż już nawet najprostsze

metody, nie wymagające dodatkowej rozbudowy sprzętu (ang. *hardware*) pozwalają na zapobieganie najczęstszym próbom fałszerstwa z wykorzystaniem wydruków, często przygotowanych sposobem “domowym”. Więcej informacji na temat testowania żywotności tęczówki Czytelnik znajdzie w [11].

4. Przesyłanie danych biometrycznych

Poszczególne bloki systemu biometrycznego przedstawione na rys. 1 mogą zawierać się w jednym urządzeniu fizycznym (ang. *stand-alone device*), jak również każdy z nich może znajdować się w innej, często odległej od pozostałych lokalizacji. Taki rozproszony system biometryczny może być szeroko stosowany jako narzędzie uwierzytelniania i znaleźć zastosowanie w wielu dziedzinach życia współczesnych, coraz bardziej “sieciowych” społeczeństw. W tym kontekście pojawiają się nowe zagrożenia, związane z koniecznością przesyłania danych biometrycznych na znaczne odległości i za pośrednictwem niezabezpieczonej sieci Internet. W zależności od architektury systemu dane zebrane przez urządzenie pomiarowe, przetworzone charakterystyki w postaci danych biometrycznych, wzorce biometryczne czy nawet pojedynczy wynik porównania dwóch charakterystyk biometrycznych mogą zostać zamienione lub skradzione w celu ponownego wykorzystania.

Najpewniejszym rozwiązaniem problemów transmisji wydaje się być szyfrowanie i podpisywanie wszelkich przesyłanych informacji. Podejście to będzie jednak skuteczne tylko w przypadku wykorzystania certyfikowanych modułów systemu, które będą mogły się wzajemnie uwierzytelniać. W innym wypadku nawet zaszyfrowane dane mogą zostać wysłane poprzez sfałszowany moduł systemu. Rozproszona architektura systemu sprawia, że ciężar kontroli autentyczności przesyłanych danych musi zostać przeniesiony z urządzenia pomiarowego na główny algorytm analizy danych lub inny serwer uwierzytelniający. Oczywiście konstruktorzy i administratorzy systemów bezpieczeństwa muszą dołożyć wszelkich starań, aby uniemożliwić kradzież danych biometrycznych. Dodatkowo jednak, należy zagwarantować istnienie mechanizmów, które nawet w przypadku kradzieży danych biometrycznych, uniemożliwią ich ponowne, nielegalne wykorzystanie.

4.1 Ponowne wykorzystanie wzorca

Wzorzec biometryczny w większości systemów ma taką samą lub podobną strukturę jak dane biometryczne używane do weryfikacji. Wykradzenie wzorca umożliwi złoczyńcy późniejsze wykorzystanie go w procesie weryfikacji. W pewnych przypadkach nawet wykradzenie zaszyfrowanego wzorca, choć uniemożliwi napastnikowi dostęp do jawnej postaci wzorca, może umożliwić jego powtórne wykorzystanie w procesie zdalnej weryfikacji. Może się to odbyć poprzez powtórne wysłanie skradzionych danych w niezmienionej postaci do modułu weryfikacji. Szczególną cechą danych biometrycznych jest jednak ich zmienność. Inaczej niż w przypadku zabezpieczeń bazujących na tradycyjnych hasłach, dane biometryczne pochodzące z różnych pomiarów tej samej charakterystyki biometrycznej (od tej samej osoby) będą się zawsze nieco różnić. Sztuka konstruowania algorytmów biometrycznej identyfikacji i weryfikacji polega m.in. na odpowiednim interpretowaniu tych zmian. Fakt ten

pozwala na zastosowanie stosunkowo prostego mechanizmu zabezpieczania systemu przed ponownym wykorzystaniem wzorca. Mechanizm ten polega na porównaniu danych biometrycznych ze wzorcem, tak jak w każdym procesie porównania danych biometrycznych, z tą jednak różnicą, że dane nie tylko nie mogą się “za bardzo” od wzorca różnić (jak w “zwykłym” procesie porównania), jak też nie mogą być “za bardzo” do niego podobne. Nadmierne podobieństwo sugeruje bowiem, iż użyto skradzionego wzorca danych biometrycznych. Metodę tę nazywamy podwójnym progowaniem.

4.2 Podsłuchanie danych biometrycznych

Podobna sytuacja może mieć miejsce, gdy transmitowane dane biometryczne zostaną podsłuchane, a potem ponownie wykorzystane do weryfikacji (ang. *biometric replay-attack*). Prosty mechanizm przeciwdziałania tego typu zagrożeniom polega na tzw. sprawdzaniu z buforowaniem. Każda próba weryfikacji oznacza w takim przypadku nie tylko porównanie bieżących danych z wzorcem, ale również z danymi użytymi do udanych weryfikacji w przeszłości i przechowywanymi w pamięci systemu. Takie rozwiązanie wydłuża niestety łączny czas weryfikacji.

Inna technika polega na parametryzacji metod uwierzytelniania. W przypadku biometrii tęczówki, system może przykładowo wymagać przesłania danych dotyczących odpowiedniego oka (lewego lub prawego) lub jedynie pewnego fragmentu (wycinka) wzoru tęczówki.

4.3 Nielegalny dostęp do podsystemu porównującego

W przypadku, gdy oszust uzyska dostęp do podsystemu porównującego wzorce z danymi biometrycznymi i ma możliwość uzyskania wyników porównania wzorca z arbitralnymi danymi może on zastosować atak typu *brute-force* lub *hill-climbing.* Ataki te polegają na generowaniu danych według pewnej sekwencji i powtarzaniu prób weryfikacji, aż do momentu uzyskania wyniku akceptującego. *Hill-climbing* jest bardziej zaawansowaną metodą wykorzystującą wiedzę o poprzednich próbach oraz metody optymalizacji. W przypadku biometrii tęczówki, gdzie zbiór cech jest kodem binarnym, atak tego typu polegałby na podmianie pojedynczych bitów i obserwacji zmiany wyniku na wyjściu. Jednym ze sposobów przeciwdziałania atakom typu *hill-climbing* jest kwantowanie wyników porównania. Ze względu na fakt, że po zastosowaniu kwantowania funkcja podobieństwa staje się nieciągła względem argumentów, utrudnia to stosowanie metod gradientowych optymalizacji. Rzeczywisty wynik porównania powinien zatem być wykorzystywany jedynie do wewnętrznych operacji podsystemu uwierzytelniającego, a poza system należy wysyłać jedynie jego dyskretną postać (binarną w przypadku weryfikacji). Dodatkowo wynik może być także przesyłany w postaci zaszyfrowanej. Należy również stosować typowe zabezpieczenia przeciw atakom typu *brute-force,* polegające na ograniczeniu liczby następujących po sobie prób weryfikacji.

4.4 Bezpieczna transmisja biometryczna – protokół BEAP.

Opisane powyżej proste metody zabezpieczeń dotyczą jedynie wybranych zagrożeń. Dopiero połączenie metod zapobiegania wszystkim rodzajom znanych ataków na wszystkich poziomach systemu (na poziomie

urządzeń, algorytmów i aplikacji oraz transmisji) może zapewnić całościową ochronę. Takie możliwości stwarza protokół BEAP (ang. *Biometric Extensible Authentication Protocol*), który został opracowany wspólnie przez Pracownię Biometrii NASK i Telefonica I+D (Hiszpania), w ramach prac europejskiego projektu badawczego BioSec. Protokół BEAP bazuje na szkielecie protokołów EAP, zdefiniowanym w RFC-3784. Protokoły rodziny EAP są obecnie szeroko wykorzystywane w sieciach bezprzewodowych (w ramach standardu 802.1X zaadaptowanego m.in. przez WPA i WPA2), jak również w połączeniach typu punkt-punkt (np. w wirtualnych sieciach prywatnych - VPN). EAP sam w sobie nie jest mechanizmem uwierzytelniania, a jedynie szkieletem dla budowania nowych protokołów.

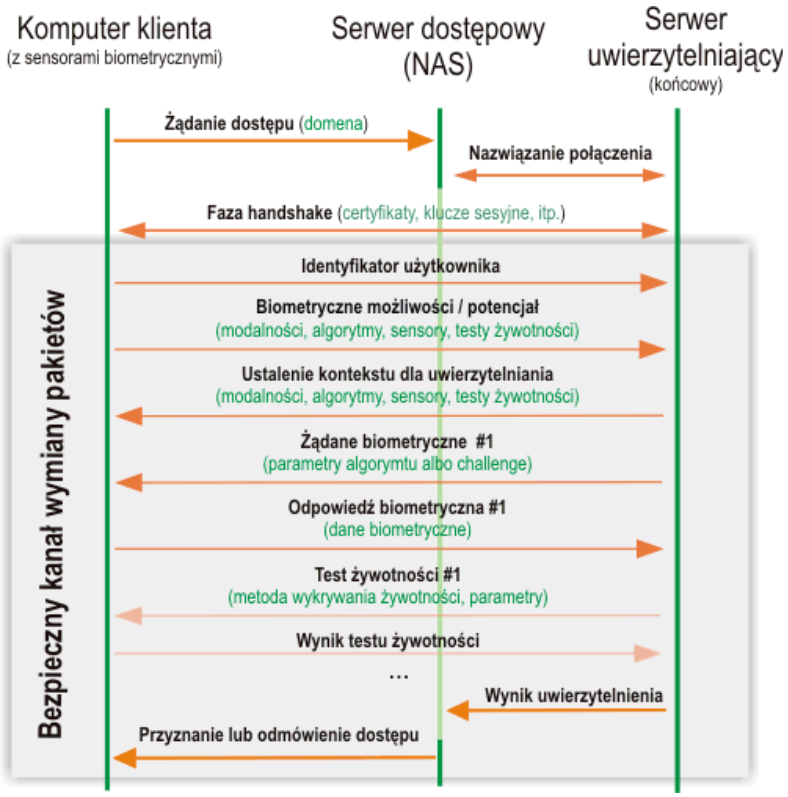
W przypadku biometrycznych metod weryfikacji, poufność przesyłanych informacji jest najwyższym priorytetem. W przeciwieństwie do standardowych metod opartych na kluczach i hasłach, podstawowych danych biometrycznych nie można unieważnić, ponieważ nie można w prosty sposób zmienić cech biologicznych i behawioralnych ich właściciela. W protokole BEAP wszystkie informacje związane z użytkownikiem są transportowane wyłącznie w zaszyfrowanej i podpisanej formie (podpis elektroniczny), po uprzedniej wymianie i sprawdzeniu certyfikatów. Dla celów bezpieczeństwa cyfrowego wykorzystywane są mechanizmy protokołu TLS, powszechnie używane do zabezpieczania transmisji w sieci Internet oraz infrastruktura klucza publicznego (PKI).

Protokół BEAP umożliwia dzielenie dużych pakietów danych na mniejsze, odpowiednio oznakowane pakiety, których rozmiar dopuszcza warstwa łącza. BEAP został także wyposażony w mechanizm oddelegowania uwierzytelniania. Proces weryfikacji nie jest wówczas przeprowadzany przez serwer dostępowy, ale przez serwer uwierzytelniający odpowiadający za daną domenę. Takie rozwiązanie pozwala na centralizację zarządzania procesem uwierzytelniania i dostępu do bazy danych biometrycznych. Niektóre rodzaje biometrii zakładają rozbudowaną interakcję systemu z użytkownikiem, który odpowiada na pewne żądania ze strony systemu. Protokół BEAP umożliwia przesyłanie wiadomości do stacji klienta, a także wspiera, opisywane powyżej, parametryzowane metody biometryczne oraz metody wielomodalne.

Proces uwierzytelniania w protokole BEAP jest procesem dwufazowym. W pierwszej fazie (ang. *handshake*), strony dokonują wzajemnej lub jednostronnej walidacji certyfikatów, w celu uwierzytelnienia urządzeń biorących udział we właściwym procesie weryfikacji tożsamości. Zapobiega to podszywaniu się pod serwer uwierzytelniający lub stację kliencką, przeciwdziałając tym samym atakom typu *man-in-the-middle*, *hill-climbing* oraz *brute-force*. W następnym kroku generowane są kryptograficzne klucze sesyjne i ustanawiany jest bezpieczny kanał transmisyjny. Wygenerowane klucze wykorzystywane są do szyfrowania i podpisywania każdego pakietu przesyłanego w dalszej części procesu uwierzytelniania. Mechanizmy pierwszej fazy realizowane są poprzez enkapsulację protokołu TLS. Specyfikacja EAP zakłada, że pierwszy pakiet wysyłany przez stronę uwierzytelnianą powinien zawierać identyfikator klienta wraz z nazwą domeny, do której klient zamierza

uzyskać dostęp. W takim przypadku przesyłanie nazwy użytkownika odbywa się w trakcie pierwszej fazy, kiedy transmitowane informacje nie są jeszcze zabezpieczone przed podsłuchem i zamianą. W niektórych zastosowaniach ochrona identyfikatora użytkownika wydaje się być uzasadniona. Z tego względu w protokole BEAP transmisja wszystkich danych związanych bezpośrednio z tożsamością osoby została przeniesiona do fazy drugiej. W sposób niezaszyfrowany przesyłana jest tylko nazwa domeny.

Druga faza jest właściwym procesem weryfikacji tożsamości klienta. W pierwszym kroku przesyłany jest identyfikator klienta. Następnie stacja klienta wysyła do serwera informacje o sensorach, w jakie jest wyposażona, o wspieranych metodach biometrycznych, algorytmach i dostępnych testach żywotności. Serwer uwierzytelniający bazując na wewnętrznej polityce bezpieczeństwa oraz informacjach pobranych z biometrycznej bazy wzorców, decyduje, jakie elementy będą wykorzystywane podczas weryfikacji i przesyła informację zwrotną. Sam proces uwierzytelniania polega na iteracyjnym wysyłaniu przez serwer kolejnych pakietów z prośbą o dane biometryczne. Pakiety te mogą zawierać parametry dla metody lub sensora oraz elementy dialogu z użytkownikiem. Dodatkowo strona uwierzytelniająca może przesyłać żądanie przeprowadzenia określonych testów żywotności. Porównywanie danych ze wzorcem dokonywane jest po stronie serwera, który jako jedyny ma bezpośredni dostęp do bazy wzorców biometrycznych. Po uzyskaniu wyniku, informacja o pozytywnej lub negatywnej weryfikacji przesyłana jest do klienta. Wynik weryfikacji jest przesyłany w ramach bezpiecznego połączenia, aby zapobiec sytuacji, w której pod koniec sesji, strona trzecia przechwytuje połączenie i wysyła fałszywy komunikat o udanej weryfikacji. Uproszczony diagram wymiany informacji podczas uwierzytelniania został przedstawiony na rys. 8.



Rysunek 8: Schemat uwierzytelniania biometrycznego w dostępie zdalnym z wykorzystaniem protokołu BEAP.

Przedstawiony scenariusz zakłada scentralizowane przechowywanie i użycie wzorców biometrycznych. Protokół BEAP przewiduje również możliwość rozszerzenia scenariusza i wykorzystania bezpiecznego przechowywania wzorców na kartach inteligentnych, tokenach lub dokumentach wyposażonych w karty zbliżeniowe. Więcej informacji na temat protokołu BEAP Czytelnik znajdzie w [7]. O bezpiecznym przechowywaniu danych biometrycznych piszemy w następnym rozdziale.

5. Przechowywanie danych biometrycznych

Klasyczne podejście do zarządzania informacją uwierzytelniającą lub danymi osobowymi zakłada istnienie centralnej bazy tych danych (oczywiście określenie “centralna baza danych” nie narzuca jej fizycznej realizacji). W wielu przypadkach takie podejście jest uzasadnione. Przykładem może tu być ewidencja obywateli kraju. Otwartą kwestią jest pytanie czy tworzenie baz danych obywateli kraju jest konieczne i etyczne. Dyskusja na ten temat wychodzi jednak poza zakres tematyczny niniejszego referatu. Ochrona biometrycznych baz danych może być realizowana w ten sam sposób jak ochrona innych baz danych zawierających dane osobowe, z uwzględnieniem dodatkowych mechanizmów zabezpieczeń dotyczących transmisji danych biometrycznych (opisanych powyżej).

Można jednak wskazać cały szereg zastosowań, istniejących i potencjalnych, w których stosowanie centralnych baz danych nie jest konieczne. Przykładem mogą być, stosowane już obecnie, biometryczne bilety

wstępu do parków rozrywki, ważne przez kilka dni. Biometria ma w wygodny sposób zabezpieczać przed korzystaniem z jednego biletu przez kilka różnych osób. W tym wypadku gromadzenie danych w centralnej bazie jest niepotrzebne. Zamiast tego mogą zostać użyte “osobiste” bazy danych w postaci np. kart inteligentnych. Każdy użytkownik wyposażony w osobistą kartę z zapisanymi na niej wzorcami biometrycznymi pozostaje wówczas jedynym “właścicielem” swoich danych biometrycznych. Co więcej, dane te są dodatkowo zaszyfrowane, a sam proces porównania odbywa się na karcie (tzw. technologia *match-on-card*), a nie w zewnętrznym systemie. Dane biometryczne więc nigdy nie opuszczają karty, a w przypadku jej utraty nie będą mogły zostać ponownie wykorzystane (wbudowane mechanizmy karty umożliwiają jedynie zapis wzorca z zewnątrz, odczyt możliwy jest tylko przez wewnętrzne mechanizmy karty bez wysyłania danych na zewnątrz). W ten sposób każdy użytkownik zawsze “wie” co dzieje się z jego danymi biometrycznymi. Takie podejście może zostać zastosowane praktycznie we wszystkich systemach weryfikacji tożsamości, gdzie centralne przechowywanie danych biometrycznych nie jest konieczne, a często motywowane czynnikami pozatechnicznymi. Ponadto okazuje się, iż utrzymywanie takiej rozproszonej bazy danych biometrycznych jest tańsze niż utrzymywanie dużej bazy centralnej. Koszt utrzymania rozproszonej bazy danych w postaci osobistych kart inteligentnych sprowadza się praktycznie do jednorazowego wyprodukowania nośnika oraz zapisania wzorców na karcie. Z drugiej strony podejście takie ogranicza wygodę użytkownika, będącą jedną z podstawowych zalet biometrii, poprzez wymuszenie na użytkowniku konieczności noszenia przy sobie dodatkowego przedmiotu. Mimo to, takie podejście może zostać stosunkowo łatwo zintegrowane z istniejącymi systemami, bez konieczności przebudowy całej infrastruktury informatycznej (co byłoby konieczne np. w przypadku całkowitej rezygnacji z kart na rzecz rozwiązań biometrycznych i w związku z tym przyjęcia architektury z centralną bazą danych).

Współcześnie produkowane karty inteligentne, mimo swoich małych rozmiarów (sam układ elektroniczny jest rozmiaru główki zapałki; wielkość plastikowej “obudowy” podyktowana jest wygodą użytkowników) są w pełni funkcjonalnymi układami z własną pamięcią, procesorem, a nawet systemem operacyjnym. Mocą obliczeniową dorównują one komputerom osobistym z lat 80-tych. Jednym z rodzajów kart inteligentnych są tzw. JavaCards, czyli karty wyposażone w wirtualną maszynę języka Java. Ta właściwość znakomicie ułatwia pisanie aplikacji dedykowanych do użycia na kartach inteligentnych. Wersja maszyny wirtualnej dla kart (tzw. JCVM – ang. *Java Card Virtual Machine*) ma jednak ograniczone możliwości, stąd przeniesienie aplikacji biometrycznych na kartę inteligentną nie jest bezpośrednie.

5.1 Bezpieczeństwo uwierzytelniania z użyciem karty inteligentnej

Scenariusz uwierzytelniania z użyciem karty inteligentnej zakłada istnienie trzech podstawowych podmiotów:

- karty,
- użytkownika (właściciela karty),
- terminala czytającego kartę (np. bankomat).

Transakcję można uznać za bezpieczną tylko wówczas, gdy każdy podmiot jest w stanie zagwarantować pozostałym, że jest tym, za kogo się podaje. Stąd wymagane są trzy etapy wzajemnego uwierzytelniania:

- karta uwierzytelnia terminal oraz terminal uwierzytelnia kartę,
- użytkownik uwierzytelnia terminal oraz terminal uwierzytelnia użytkownika,
- karta uwierzytelnia użytkownika oraz użytkownik uwierzytelnia kartę.

Wzajemne uwierzytelnianie karty i terminala odbywa się poprzez zastosowanie mechanizmów kryptograficznych. Karta wysyła do terminala losowy ciąg danych i prosi o zaszyfrowanie go tajnym kluczem, który znają tylko autoryzowane terminale oraz karta. Karta porównuje szyfrogram wygenerowany przez terminal z własnym szyfrogramem i na tej podstawie stwierdza wiarygodność terminala. W analogiczny sposób terminal sprawdza wiarygodność karty. Dalsza komunikacja między kartą a terminalem może być, jeśli są takie wymagania, zabezpieczona podpisem oraz szyfrowana.

Należy zwrócić uwagę, że karta która uwierzytelniła terminal nie ma możliwości poinformować o tym użytkownika. Proste rozwiązanie tego problemu, polega na umieszczeniu pewnego prywatnego komunikatu na karcie. Dopiero po udanym uwierzytelnieniu komunikat może zostać przez kartę odblokowany i wyświetlony w oknie terminala. Jest to element uwierzytelniania terminala przez użytkownika. Pozwala to zapobiegać takiej sytuacji, w której fałszywy terminal wyświetla komunikat z prośbą do użytkownika o dokonanie pomiaru biometrycznego, w celu kradzieży danych biometrycznych. Etap uwierzytelniania użytkownika przez terminal może zostać pominięty. Terminal “ufa” karcie, która uwierzytelnia użytkownika i bazuje na informacji przekazanej przez kartę.

Tradycyjnie proces uwierzytelniania użytkownika przez kartę polega na podaniu numeru identyfikacyjnego PIN. Ta metoda może zostać zastąpiona poprzez weryfikację biometryczną, która odbywa się całkowicie na pokładzie karty inteligentnej. Etap uwierzytelnienia karty przez użytkownika może odbywać się w oparciu o ten sam mechanizm, przy pomocy którego użytkownik uwierzytelnia terminal, tzn. poprzez wyświetlenie na ekranie terminala prywatnego komunikatu, znanego tylko właścicielowi karty. Wyświetlenie prawidłowego komunikatu potwierdza, że zarówno terminal, jak i karta nie zostały sfałszowane. W wielu sytuacjach można zastosować niejawny mechanizm uwierzytelniania karty przez użytkownika. Mechanizm ten jest *de facto* stosowany powszechnie w dzisiejszych systemach wykorzystujących karty – osoba korzystająca z karty przez fakt jej posiadania i chęć użycia uwiarygadnia tę kartę. Aby ten prosty mechanizm był dostatecznie pewny wzór karty nie może być łatwy do podrobienia.

5.2 Biometria i karty inteligentne – efektywność i ograniczenia

Karty inteligentne w obecnym stadium zaawansowania technologicznego nakładają pewne ograniczenia, które muszą być brane pod uwagę przy tworzeniu systemów biometrycznych wykorzystujących karty. W zależności od potrzeb, system może zostać zoptymalizowany pod kątem szybkości działania, zużycia pamięci karty lub też dokładności weryfikacji biometrycznej. Dla

opisywanej powyżej metody weryfikacji tożsamości w oparciu o wzór tęczówki oka, w zależności od przyjętego podejścia, czas weryfikacji na karcie waha się od 2 do 15 sekund, a zużycie pamięci karty od 0,5% do 25% całkowitej pojemności pamięci. Wielkość zużywanej pamięci może mieć znaczenie, ze względu na konieczność umieszczenia na karcie dodatkowych informacji, wymaganych przez konkretne zastosowania. Zestawienie danych dotyczących wykorzystania zasobów karty i procesu weryfikacji na karcie przy użyciu biometrii tęczówki przedstawia tab. 1.

Tabela 1: Ocena wariantów weryfikacji tęczówki wykonywanej przez kartę inteligentną ze względu na podstawowe wymagania systemu

Czynnik optymalizowany	Zużycie pamięci karty	Średni czas weryfikacji
Szybkość działania	5-25%	3-5 s.
Dokładność weryfikacji	5-25%	13-15 s.
Zużycie pamięci karty	0,5-1,5%	12-14 s.

We wszystkich konfiguracjach największą część czasu zabiera proces komunikacji pomiędzy kartą a terminalem. Można mieć nadzieję, że w miarę rozwoju technologii to ograniczenie będzie stawało się coraz mniej istotne. Już na obecnym stadium zaawansowania, karty zoptymalizowane pod kątem szybkości działania mogą znaleźć liczne zastosowania praktyczne. Przygotowany schemat użycia uwierzytelniania biometrycznego na kartach inteligentnych może także zostać łatwo wykorzystany w telefonach komórkowych (karty SIM) czy urządzeniach typu PDA. Więcej informacji na temat zastosowania kart inteligentnych w połączeniu z biometrią Czytelnik znajdzie w [6,13].

LITERATURA

[1] DUBISZ Stanisław (red.): *Uniwersalny Słownik Języka Polskiego.* Wydawnictwo Naukowe PWN SA. Warszawa 2003.
[2] BOWMAN Erik: *Everything You Need To Know About Biometrics.* Identix Corporation 2000.
[3] DENNING Dorothy: *Wojna informacyjna i bezpieczeństwo informacji.* Wydawnictwa Naukowo-Techniczne. Warszawa 2002.
[4] CZAJKA Adam: *Human iris for automatic identity verification.* Rozprawa doktorska. Politechnika Warszawska. Warszawa 2005.
[5] CZAJKA Adam, PACUT Andrzej: *Biometria tęczówki oka,* w ZAJĄC Paweł, KWAŚNIOWSKI Stanisław (red.): *Automatyczna identyfikacja w systemach logistycznych,* str. 214-228. Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław 2004.
[6] STRZELCZYK Przemysław, CHOCHOWSKI Marcin: *Inteligentne karty biometryczne.* Biuletyn NASK nr 3/2005. Warszawa 2005. http://www.nask.pl/run/n/Biuletyn
[7] STRZELCZYK Przemysław: *Protokół BEAP.* XXII Krajowe Sympozjum Telekomunikacji i Teleinformatyki. Bydgoszcz 2006.

[8] THALHEIM Lisa, KRISSLER Jan, ZIEGLER Peter: *Biometric Access Protection Devices and their Programs Put to the Test. c*'t 11/2002. http://www.heise.de/ct/english/02/11/114/

[9] DAUGMANN John: *Countermeasures against Subterfuge,* w JAIN Anil, PANKANTI Sharath, BOLLE Ruud (red.): *BIOMETRICS: Personal Identification in Networked Society.* Kluwer Academic Publishers. Amsterdam 1999.

[10] DAUGMANN John: *Anti-spoofing Liveness Detection,* artykuł dostępny online: http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf

[11] PACUT Andrzej, CZAJKA Adam: *Aliveness detection for iris biometrics.* Konferencja Carnahan 2006. Lexington, USA (w druku).

[12] CLYNES Manfred, KOHN Michael: *Color dynamics of the pupil.* Annuals of N.Y. vol. 156, Academy of Science 1967

[13] STRZELCZYK Przemysław, CHOCHOWSKI Marcin, PACUT Andrzej, CZAJKA Adam: *Biometryczna karta elektroniczna.* Konferencja Secure 2005. http://www.secure.edu.pl/historia/2005/prezentacje2005.html

[14] WARDZIŃSKI Rafał: *Emerging biometrics: person identification from EEG.* XVIII Joint IEEE-SPIE Symposium Wilga. Wilga 2006 (w druku).

[15] PACUT Andrzej, CZAJKA Adam: *Iris Aliveness Detection.* BioSec 2nd Workshop. Bruksela, 20 stycznia 2005.