

## Biometryczne uwierzytelnianie rozmówców telefonicznych

**Liczba kradzieży tożsamości rośnie niezwykle szybko. Gartner Group twierdzi, że między rokiem 2003 i 2004 liczba takich przypadków wzrosła o 80%. W 2004 roku 9,3 miliona Amerykanów było ofiarami kradzieży tożsamości, a firmy straciły ponad 50 miliardów dolarów (Better Business Bureau). Technologia, która może pomóc w zwalczaniu tego zjawiska wyszła z fazy badań i zaczęła być dostępna komercyjnie.**

### Kradzież tożsamości

Dzięki zdobyciu kilku podstawowych informacji, takich jak numer karty kredytowej, daty urodzenia, adresu, nazwiska panińskiego matki, numeru PESEL lub PINu, osoba podszywająca się pod inną osobę może przekonać instytucję (np. bank), że ma prawo do użycia rachunku bankowego lub karty kredytowej. Przestępca podaje się za inną osobę i korzysta z jej uprawnień.

### Tradycyjne sposoby przeciwdziałania kradzieży tożsamości

Tradycyjne sposoby przeciwdziałania kradzieży tożsamości obejmują identyfikację i uwierzytelnianie nie osoby, ale numeru, hasła, karty magnetycznej lub mikroprocesorowej. Wszystkie te identyfikatory narażone na zgubienie, kradzież lub skopiowanie. Są zwykle stosunkowo kosztowne i zawodne. Według Gartner Group, 25–30% rozmów z help deskami dotyczy problemów z hasłem. Gartner szacuje, że zmiana haseł jednego użytkownika kosztuje 10–30 dolarów rocznie.

Hasła i PINy, numery umów, numery klienta doprowadzają użytkowników do rozpacz. Niewiele banków daje możliwość zmiany PINu na bardziej przyjazny. Każdy z nas nosi w portfelu kilka kart, a każda z nich ma inny PIN. Gubimy się wciskając błędne PINy, złościmy gdy musimy odblokowywać karty, ponieważ trzy razy wybraliśmy zły kod dostępu.

### Biometryczne metody rozpoznawania i identyfikowania osób

Biometryczne metody rozpoznawania i identyfikowania osób dokonywane są na podstawie cech fizycznych (charakterystyki linii papilarnych, kształtu twarzy, geometrii dłoni, wzoru tęczy oka) i behawioralnych (pisma ręcznego, mowy, sposobu uderzania w klawisze). Różnią się one między sobą podatnością na podrobienie. Wszystkie jednak charakteryzują się tym, że nie sposób ich ukraść.

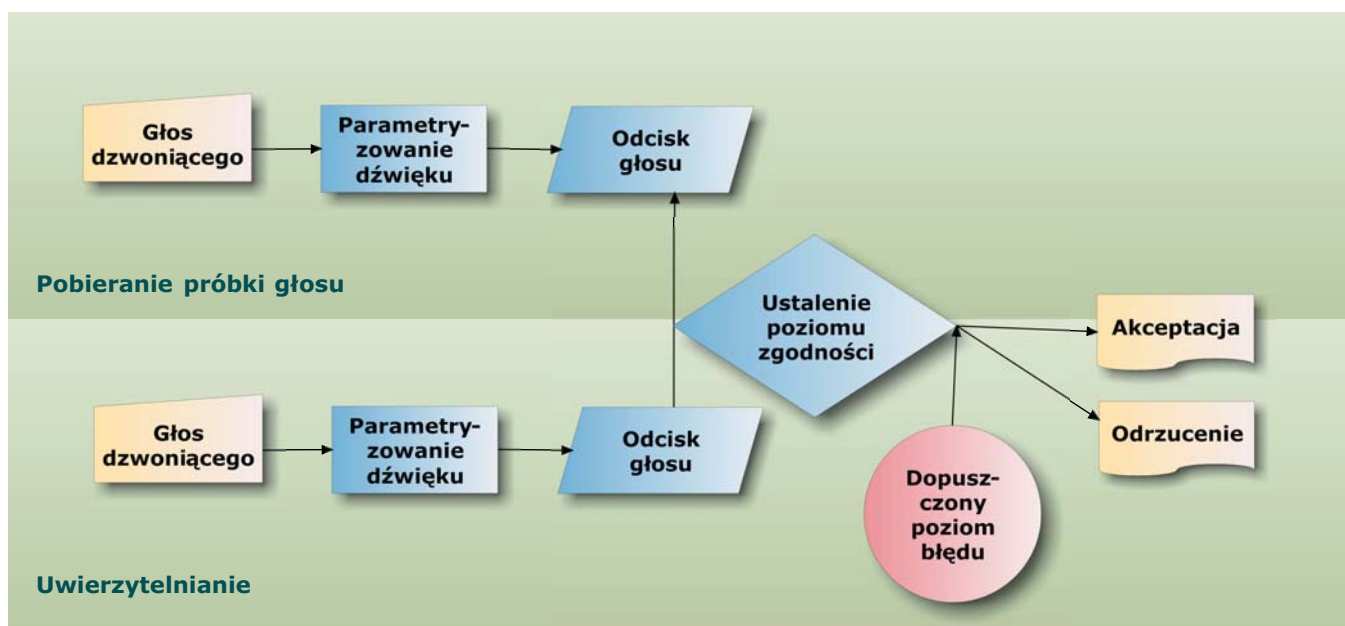
Informacja przetwarzana i przesyłana w systemach biometrycznych jest całkowicie niedostępna dla osób postronnych. Ma ona bowiem charakter matematycznego zapisu cech charakterystycznych. Dodatkowo dane te są szyfrowane, podobnie jak szyfrowana jest ich transmisja. Tak więc dane chronione są zarówno przed przypadkowym, jak i celowym działaniem intruzów.

# Autoryzowanie na podstawie głosu

Biometryczne metody identyfikacji głosu i autoryzacji są wykorzystywane do uniemożliwienia nieautoryzowanych prób dostępu do bankomatów, komputerów osobistych, sieci komputerowych, telefonów komórkowych, domowych systemów alarmowych itd. Mogą one być stosowane zarówno oddzielnie jak i łącznie z tradycyjnymi metodami identyfikacji i uwierzytelniania.

Autoryzowanie na podstawie głosu ma to do siebie, że nie wymaga żadnych urządzeń sprawdzających po stronie użytkownika. Odbywa się ono w czasie zwyczajnej rozmowy telefonicznej.

## Proces uwierzytelniania dzwoniącego



Marian J. Kostecki, opr. własne na podstawie PerSay.com

Najpierw musi zostać pobrana próbka głosu. Odbywa się to zwykle w ten sposób, że po wyrażeniu zgody na dodanie tego dodatkowego poziomu bezpieczeństwa, klient trzykrotnie powtarza ustaloną wcześniej sekwencję cyfr, słów lub fraz. Pobrane, czyli zarejestrowane (nagrane) próbki głosu, są następnie parametryzowane, opisywane za pomocą ponad 30 różnych cech. Tym, co przechowywane jest na serwerze, na którym dokonywane są operacje biometrycznej identyfikacji głosu, to pliki z parametrami, a nie pliki dźwiękowe.

Inną opcją jest próbka głosu niezwiązana z żadnym tekstem. Próbki pobiera się w czasie trzech kolejnych rozmów telefonicznych. Wystarczy nagranie o łącznej długości ok. 30 sekund, aby przygotować „odcisk głosu” i posługiwać się nim później dla celów uwierzytelniania dzwoniącego.

Każda próba późniejszego uwierzytelniania, polegająca na porównaniu głosu dzwoniącego z „odciskiem głosu” wrażana jest wynikiem liczbowym, wskazującym na poziom podobieństwa obu pomiarów.

Dokładność biometrycznej charakterystyki głosu, tak jak dokładność każdego innego pomiaru, może być scharakteryzowana przy pomocy dwóch zmiennych: błędnego zaakceptowania i błędnego odrzucenia. Błędna akceptacja, to błąd polegający na potraktowaniu oszusta jak osoby uprawnionej, a błędne odrzucenie, to błąd polegający na potraktowaniu osoby uprawnionej jak oszusta.

Uwierzytelnienie dotyczące dostępu do bardzo istotnych danych lub działań o dużych konsekwencjach wymaga ustawienia błędnej akceptacji na wysokim poziomie. Każdy błąd w tej materii może być bowiem bardzo kosztowny. Przy dużych operacjach giełdowych dokonywanych przez telefon pobiera się zwykle wiele próbek, aby ograniczyć możliwość wystąpienia tego błędu. Przy operacjach bankowych polegających na przelewaniu niewielkich kwot z konta oszczędnościowego na rachunek bieżący wymagania dotyczące dokładności pomiaru nie muszą być tak wysokie.

Dokładność biometrycznej charakterystyki głosu zależna jest od kilku czynników, w tym czasu trwania (długości) próbek głosu, liczby pobranych odcisków, hałasu w tle. Zwykle przeziębienie zwykle nie zaburza biometrycznej charakterystyki głosu, choć zapalenie krtani może ją poważnie zaburzyć.

Konieczność pobierania trzech niezależnych od wygłaszanego tekstu próbek w trakcie trzech oddzielnych rozmów bierze się stąd, że nasz głos zmienia się w zależności od pory dnia, od naszego samopoczucia, emocji (zdenerwowania, radości), czy wreszcie aparatu telefonicznego z którego prowadzona jest rozmowa.

Doskonała zgodność „odcisku głosu” i próbki pobranej w czasie rozmowy świadczyć może o tym, że podczas rozmowy zostało wykorzystane nagranie głosu. Stąd ta doskonała zgodność dyskwalifikuje dzwoniącego.

## Gdzie to już działa

Holenderska policja miała poważne problemy z kibicami-chuliganami. Osobnik, który znalazł się na takiej liście, musiał tuż przed meczem meldować się na posterunku policji, co miało zagwarantować jego nieobecność na stadionie. Teraz ma jedynie obowiązek być w domu. IVR, do którego podłączony jest system biometrycznego uwierzytelniania głosu, dzwoni na jego numer domowy. Jeżeli słuchawkę podniesie ów osobnik, wiadome staje się, że jest w domu i najprawdopodobniej ogląda mecz. Policjanci także mogą spokojnie mecz oglądać.

Podobnym celom służy weryfikacja głosu w amerykańskim Ministerstwie Bezpieczeństwa (Department of Homeland Security, Immigration Control & Enforcement). Do niedawna wybrane grupy imigrantów w niektórych stanach miały obowiązek meldowania się w urzędzie. Teraz w 22 stanach i pobyt pod zadeklarowanym adresem sprawdza IVR i system weryfikacji głosu.

Pracownicy administracji miasta Jerozolima są ulokowani w dziesiątkach miejsc. Po przyjeździe do pracy wdzwaniamy się do systemu, który potwierdza ich obecność.

Amerykański Banner Health zarządza szpitalami w siedmiu zachodnich stanach USA. Dane dotyczące zdrowia milionów pacjentów muszą być szczególnie chronione przed dostępem ze strony nieupoważnionych osób. Dostęp do nich ze strony 25 tysięcy pracowników Banner Health jest chroniony systemem biometrycznego uwierzytelniania dzwoniących.

Pracownicy wielkich amerykańskich banków inwestycyjnych Morgan Stanley i Lehman Brothers muszą się ze sobą komunikować, a to o czym rozmawiają, to całkiem często wysoce poufne informacje. System biometrycznego uwierzytelniania dzwoniących stroi na straży bezpieczeństwa uczestników telekonferencji prowadzonych przez pracowników tych banków.

Izraelski bank Leumi, jak wiele innych banków, ma wśród swoich klientów także klientów specjalnych, obsługiwanych przez prywatnych doradców. Prywatny doradca nie ma zwykle żadnych problemów i ustaleniem, że osoba z którą rozmawia, to właśnie ten specjalny klient. Kłopoty zaczynają się wtedy,

gdy prywatny doradca zachoruje, weźmie wolny dzień lub pójdzie na urlop. Inny pracownik banku musi na początku rozmowy poddać klienta skomplikowanemu przesłuchaniu ustalającemu, że jest on tą osobą za którą się podaje. System biometrycznego uwierzytelniania dzwoniących pozwala zidentyfikować rozmówcę bez irytowania go.

W British Telecom system biometrycznego uwierzytelniania dzwoniących chroni dostęp do portali finansowych, związanych z podróżami i gramami.

Największy system biometrycznego uwierzytelniania dzwoniących działa w Bell Canada. W ciągu pierwszych 12 tygodni pobrano tam 250 000 „odcisków głosu” i liczba ta rośnie każdego dnia.

## A u nas?

Przynajmniej dwa banki, jeden holenderski i jeden irlandzki, będące właścicielami polskich banków, prowadzą zaawansowane testy biometrycznego uwierzytelniania dzwoniących. To sygnał, że technologia ta może już niebawem trafić do Polski kanałami wewnątrz-korporacyjnymi.

Jako klient banków, firm telekomunikacyjnych, telewizji kablowej i wszystkich innych, które w kontakcie z nimi wymagają abym pamiętał nadane mi unikalne identyfikatory, po cichu życzę sobie aby jak najszybciej znalazły sposób na uwolnienie mnie od tego kłopotu. System biometrycznego uwierzytelniania dzwoniących wydaje się być dobrą alternatywą.

---

Marian J. Kostecki, szef MasterPlanu – firmy doradczo szkoleniowej działającej w branży call center/help desk. Prezes Stowarzyszenia Managerów Call Center. Autor *Poradnika Telemarketera* (1997), *Telefonicznej rozmowy handlowej* (2006), *Efektywności i skuteczności w call center* (2007) oraz zawierającego 1155 polsko- i anglojęzycznych terminów *Glosariusza terminologii call center/help desk* (2007).

Glosariusz specjalistycznej terminologii związanej z systemami biometrycznego uwierzytelniania dzwoniących możesz ściągnąć gratis z witryny [www.masterplan.pl](http://www.masterplan.pl).

Kontakt w sprawie aktualnej listy polskich integratorów zajmujących się biometrycznym uwierzytelnianiem rozmówców: [kostecki@masterplan.pl](mailto:kostecki@masterplan.pl).

(tekst przygotowany 23 września 2007)