

INTELIĞENTNE SYSTEMY UWIERZYTELNIANIA

dr hab. inż. Mariusz Kubanek, prof. PCz

mariusz.kubanek@icis.pcz.pl

Katedra INFORMATYKI

Wykład 12

Uwierzytelnianie na podstawie cech behawioralnych

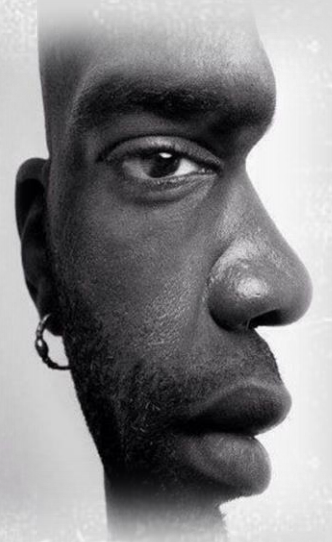
ANALIZA BEHAWIORALNA

- Samo pojęcie biometrii i uwierzytelnienia na jej podstawie jest nam dobrze znane.
- Związane jest to z potwierdzaniem naszej tożsamości indywidualnymi cechami fizycznymi, takimi jak skany linii papilarnych, skany tęczówki oka czy skan całej twarzy.
- Pojęcie analizy behawioralnej, czyli tak zwanej UBA (z ang. User Behavior Analysis) znane jest z systemów bezpieczeństwa opartych o uczenie maszynowe.



ANALIZA BEHAWIORALNA

- **Polega to na budowaniu profili standardowych postępowań użytkowników w określonym środowisku, analizowaniu wszystkich czynności, które osoba wykonuje oraz alarmowaniu, jeśli zachowanie odbiega od normy.**
- **Biometria behawioralna jest połączeniem tych dwóch pojęć.**
- **Jest to analiza behawioralna niektórych cech użytkownika.**



ANALIZA BEHAWIORALNA

- Chodzi tutaj o czynności, które wykonujemy podczas interakcji z komputerem.
- Sposób pisania na klawiaturze, prędkość kursora, krzywa tworzona podczas ruchu myszą czy nawet sposób dotykania ekranu na smartfonie.
- Wszystkie z tych czynności są dla każdego z nas unikalne i odpowiednio analizowane mogą posłużyć jako poświadczenia tożsamości.



ZALETY BIOMETRII BEHAWIORALNEJ

- Jedną z najważniejszych zalet biometrii behawioralnej jest to, że działa ona w czasie rzeczywistym, przez cały czas trwania sesji użytkownika.
- Wzorce postępowania analizowane są cały czas, podczas wpisywania znaków z klawiatury, ruchów muszą, klikania na przyciski itp.
- Jest to tak zwane uwierzytelnianie ciągłe.



ZALETY BIOMETRII BEHAWIORALNEJ

- Aby porównać to z tradycyjnymi metodami, dla przykładu odcisku palca musielibyśmy cały czas trzymać nasz palec na czytniku, aż do momentu wylogowania.
- Kolejną zaletą jest oczywiście prostota korzystania.
- Metoda nie wymaga żadnej interakcji z użytkownikiem.



ZALETY BIOMETRII BEHAWIORALNEJ

- Nie musimy pamiętać haseł, wpisywać kodów z telefonu czy skanować naszych palców.
- Po prostu korzystamy z serwisu, a system sprawdza naszą tożsamość.
- Jeśli coś jest nie w porządku i wykryte zostaną anomalie, a odpowiedni próg punktowy (scoring) zostanie przekroczony, to nastąpi wylogowanie z konta i powiadomienie użytkownika na maila.



ZALETY BIOMETRII BEHAWIORALNEJ

- Metoda oczywiście dedykowana jest bankom i specjalnie przystosowana do sprawdzania wykonywanych transakcji bankowych.
- Wydaje się, że niemożliwa jest w tym wypadku kradzież poświadczeń i użycie ich do podszycia się pod użytkownika.
- Atakujący musieliby wtedy nagrać zachowanie myszy oraz klawiatury przy wykonywaniu przelewu, odpowiednio je zmodyfikować i odtworzyć.



ZALETY BIOMETRII BEHAWIORALNEJ

- Akcja bardzo trudna do wykonania.
- Kolejny aspekt takich poświadczeń to fakt, że nie da się ich przekazać osobom trzecim.
- W przypadku haseł, pin-u, kodów czy wszystkiego innego co użytkownik podaje świadomie, jest możliwość wyłudzenia lub po prostu dobrowolnego przekazania innym osobom, aby zrobiły przelew w banku za nas.



ZALETY BIOMETRII BEHAWIORALNEJ

- Jest to wysoce niepożądane działanie, ale niestety wiele osób stosuje takie praktyki i dzieli się swoimi poświadczeniami z innymi.
- Profilu behawioralnego nie da się przekazać, nikt nie użyje klawiatury czy myszki w taki sam sposób jak my.
- To zdecydowanie dodatkowa zaleta.



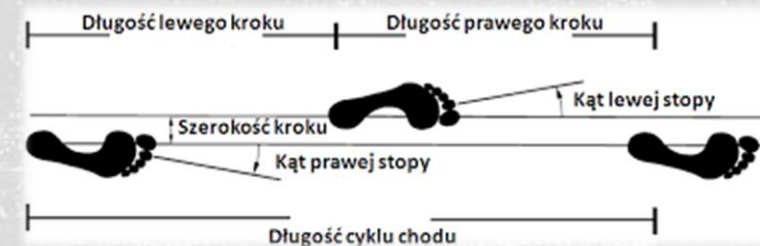
BIOMETRIA CHODU

- Biometria chodu to identyfikowanie człowieka na podstawie sposobu poruszania się.
- Analizie poddawane są elementy biomechaniki chodu, takie jak długość i szerokość kroku, kąt układania stopy, nacisk przy stawianiu kroku czy ciężar ciała.



BIOMETRIA CHODU

- Do tego dochodzi analiza obrazu ścieżki chodu, czyli „ichnogram” i wynikające z niego unikatowe cechy, takie jak kierunek i linia chodu, zmiany tempa czy anomalie ruchowe.
- Wykorzystanie biometrii chodu może być przydatne np. w udoskonalaniu systemów bezpieczeństwa w budynkach użyteczności publicznej, na lotniskach czy w obiektach takich jak stadiony lub hale koncertowe.



DYNAMICZNE PISANIE

- **Uwierzytelnianie na podstawie dynamicznego pisania na klawiaturze jest zautomatyzowaną metodą badania sposobu uderzania klawiszy na klawiaturze przez określoną osobę.**
- **Technologia bada taką dynamikę jak prędkość i nacisk, całkowity czas potrzebny na wpisanie określonego hasła, oraz czas jaki upływa pomiędzy uderzeniami klawiszy - czas wymiany (czas przez jaki przyciskamy każdy klawisz), a także czas zmiany (czas przemieszczania się pomiędzy klawiszami).**



DYNAMICZNE PISANIE

- Parametry te, pobierane w trakcie kilkunastu sesji logowania, tworzą pomiar rytmu, który jest unikatowy dla każdego użytkownika.
- Technologia pomiaru dynamiki uderzania w klawisze jest w dalszym ciągu opracowywana w celu usprawnienia solidności oraz charakteru odróżniającego.



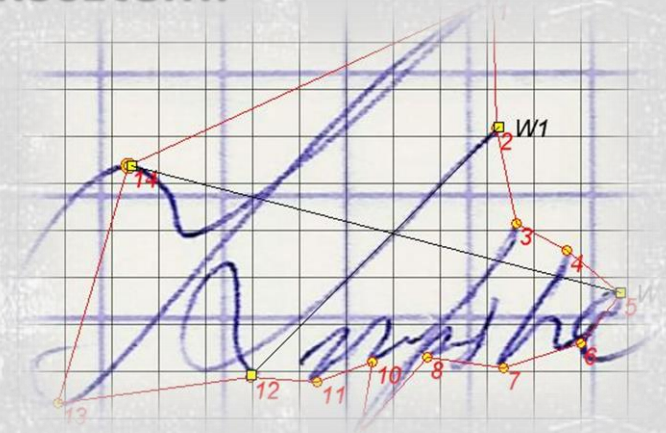
DYNAMICZNY PODPIS

- **Uwierzytelnianie na podstawie analizy dynamicznego podpisu jest to zautomatyzowana metoda analizowania podpisu określonej osoby.**
- **Technologia ta bada dynamikę, np. szybkość, kierunek oraz nacisk w trakcie pisania: czas w którym rysik pozostaje w kontakcie z papierem, całkowity czas potrzebny na złożenie podpisu oraz miejsca na papierze w którym rysik jest podrywany i opuszczany.**



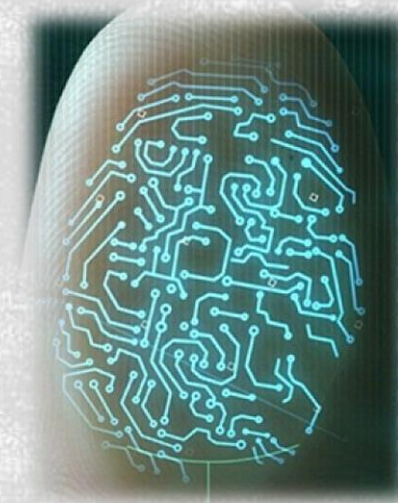
DYNAMICZNY PODPIS

- **Wzorce weryfikacji podpisu mają na ogół od 50 do 300 bajtów.**
- **W rozwiązaniach weryfikacji podpisu kluczowym elementem jest rozróżnienie pomiędzy częściami podpisu, które są charakterystyczne oraz tymi, które różnią się niemal przy każdym składaniu podpisu.**
- **Wady tego systemu obejmują problemy z długoterminową wiarygodnością, brakiem dokładności oraz znacznym kosztem.**



BEZPIECZEŃSTWO BIOMETRII

- Według wielu ekspertów w dziedzinie cyberbezpieczeństwa za kilka lat przejdziemy prawdziwą rewolucję i uwierzytelnianie ciągłe za pomocą biometrii behawioralnej będzie używane w każdym banku.
- Jest to zdecydowanie krok na przód w kierunku bezpieczniejszego korzystania z płatności internetowych.



BEZPIECZEŃSTWO BIOMETRII

- To, czy metoda ta spowoduje porzucenie korzystania z haseł i pinów okaże się w dalszej przyszłości.
- Na początku z pewnością będzie jedynie kolejnym stopniem zabezpieczenia i poświadczania naszej tożsamości.



Projekt finansowany w ramach programu Ministra Nauki i Szkolnictwa Wyższego pod nazwą „Regionalna Inicjatywa Doskonałości” w latach 2019 - 2023 nr projektu 020/RID/2018/19 kwota finansowania 12 000 000 PLN

Dziękuję za uwagę

dr hab. inż. Mariusz Kubanek, prof. PCz

mariusz.kubanek@icis.pcz.pl

Katedra INFORMATYKI