Politechnika Częstochowska

KI

INTELIGENTNE SYSTEMY UWIERZYTELNIANIA

dr hab. inż. Mariusz Kubanek, prof. PCz
mariusz.kubanek@icis.pcz.pl
Katedra INFORMATYKI

Politechnika Częstochowska

KI

Wykład 4
Rodzaje i analiza błędów w systemach uwierzytelniania tożsamości

RODZAJE BŁĘDÓW

- Każdy programista powinien mieć wiedzę na temat błędów, z którymi należy się liczyć podczas projektowania systemów biometrycznych.

- W dużej mierze skuteczność funkcjonowania systemów biometrycznych oraz innych systemów bazujących na przetwarzaniu obrazu, dźwięku, czy też innych sygnałów, jak np. systemów sterujących (w tym systemów czasu rzeczywistego) zależy od zastosowanej metody, od warunków w jakich przeprowadza się badanie, a także wstępnego przetwarzania.

RODZAJE BŁĘDÓW

- Użyty sprzęt i zastosowane algorytmy to nieodzowne atrybuty wpływające na opis poprawności działania całej aplikacji.

- Systemy biometryczne, szczególnie te wykorzystujące moduły informatyczne są podatne na błędy. Błędy takie podzielić można na:

  - błędy związane z ograniczoną ilością informacji,
  - błędy związane z odwzorowaniem cechy biometrycznej,
  - błędy związane ze zmiennością cech.

OGRANICZONA ILOŚĆ INFORMACJI

- Ilość informacji wykryta przez system biometryczny jest zależna od rodzaju sprawdzanej cechy, jakości skanera czy nawet sposobu w jaki danej osobie pobrano cechę biometryczną.

- Przykładowo ilość informacji dostarczonych przy skanie tęczówki będzie znacznie większa niż ilość informacji dostarczona przy skanie geometrii dłoni, przez co w tym drugim przypadku istnieje większe prawdopodobieństwo błędu.

OGRANICZONA ILOŚĆ INFORMACJI

- Ponadto mogą występować problemy, jeżeli wzorzec został utworzony dla innej części cechy biometrycznej niż aktualnie pobrana (co może się wiązać z np. innym przy łożeniem palca do skanera).

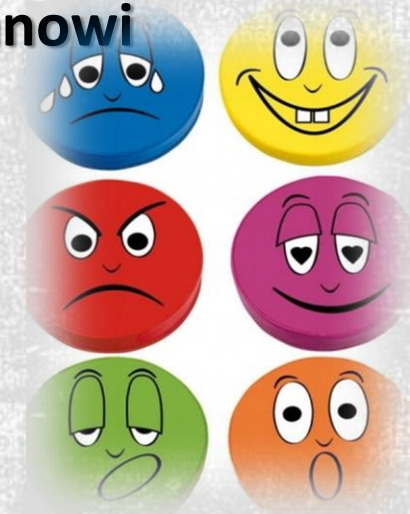
- Do limitu, czy tez kompletnego braku informacji może też dojść, jeżeli ktoś nie posiada danej cechy biometrycznej np. na skutek wypadku

ODWZOROWANIE CECHY

- Wiarygodność systemu może zostać zachwiana również podczas samej akwizycji danych od badanego.
- Najlepszym przykładem będzie badanie linii papilarnych całej dłoni.
- Skaleczenia, brud, stan zdrowia badanego, siła docisku dłoni, przebarwienia, kontuzje, uszkodzenie sprzętu lub próbki, niekorzystne warunki (np. zbyt mało światła) wszystko może sprawić ze wskazania systemu będą błędne

ZMIENNOŚĆ CECH

- Systemy biometryczne są bardzo podatne błędy związane z zmiennością organizmu ludzkiego.
- Wystarczy katar albo chrypa aby system identyfikujący na bazie głosu miał problemy z weryfikacją.
- Pracuje się nad tym żeby algorytmy były adaptacyjne, jednak stanowi to wciąż duże wyzwanie



BŁĘDY MODUŁÓW

- **Powyższe błędy wynikają z problemów, jakie występują na poziomie poszczególnych modułów systemu biometrycznego:**

- pobranie danych,
- wyodrębnianie cech,
- tworzenie wzorca.

POBRANIE DANYCH

- Skanery działające w trybie automatycznym będą najczęściej oczekiwać w trybie niskiego poboru mocy do czasu, aż w ich zasięgu znajdzie się dana cecha biometryczna wymagająca sprawdzenia.

- Mogą tutaj wystąpić dwa rodzaje błędów: FTD (ang. Failure To Detect - detekcja nieudana), ten błąd występuje w przypadku, gdy skaner nie wykryje obecności danej cechy biometrycznej (np. nie zarejestruje przyłożenia odcisku palca);

POBRANIE DANYCH

- FTC (ang. Failure To Capture - Pobieranie Nie Udane), ten błąd występuje, kiedy skaner wykryje konieczność pobrania cechy biometrycznej, ale nie będzie w stanie tego dokonać.

- Najczęściej wiąże się to z zabrudzeniem skanera lub złym ustawieniem użytkownika, uniemożliwiającym poprawne pobranie danej cechy (np. niepoprawne ułożenie dłoni/palca na skanerze)

WYODRĘBNIANIE CECH

- Po przechwyceniu cechy biometrycznej jest ona wysłana do tego modułu w celu wyodrębnienia cech szczególnych.
- Pojawić się może błąd określany jako FTP (ang. Failure To Process - wyodrębnianie nieudane).
- Błąd ten oznacza, że nie udało się wszystkich cech, które są związane z danym identyfikatorem biometrycznym.
- Błędy FTD można często spotkać w połączeniu z błędami FTP jako błędy FTA (ang. Failure To Acquire - nabycie cech nieudane).

WYODRĘBNIANIE CECH

- Niestety zbyt duży błąd FTA w znacznym stopniu zmniejsza wydajność systemu biometrycznego a dodatkowo zwiększa frustrację użytkowników.

- W celu obniżenia poziomu błędów FTA stosuje się bardziej czułe metody przechwytywania i wyodrębniania cech szczególnych, co jednak prowadzi do zwiększenia wymagań sprzętowych i czasu odpowiedzi, a także może odbić się negatywnie na działaniu dalszych modułów, jak choćby na module dopasowania.

TWORZENIE WZORCA

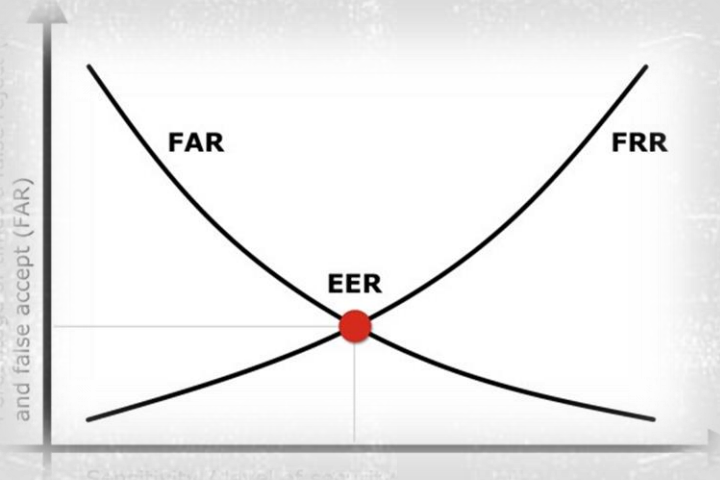
- Podczas tej czynności dla każdej cechy biometrycznej generowany jest pewien wynik z przedziału od 0 do 1.
- Wynik w pobliżu wartości 1 wskazuje na bardzo duże prawdopodobieństwo zgodności porównywanych cech.
- Uzyskanie prawdopodobieństwa wynoszące dokładnie 1 jest niewielkie, dlatego wprowadza się wartości graniczne t pozwalające na grupowanie uzyskiwanych wyników.

TWORZENIE WZORCA

- Wyniki równe lub większe od zadanego progu uznawane są za zgodne, natomiast te poniżej zadanego progu za niezgodne.

- Wyróżnić można w tym module dwa główne typy błędów:

  - błędne dopasowanie (FAR, ang. False Acceptance Rate),
  - błędne niedopasowanie (FRR. ang. False Rejection Rate).



BŁĘDNE DOPASOWANIE

- **Błędne dopasowanie – pojawia się, kiedy system uzna za zgodne dwie różne próbki, pochodzące od różnych identyfikatorów biometrycznych.**

- **Błąd ten wyrażany jest za pomocą wskaźnika FMR (ang. False Match Rate – wskaźnik błędnego dopasowania)**

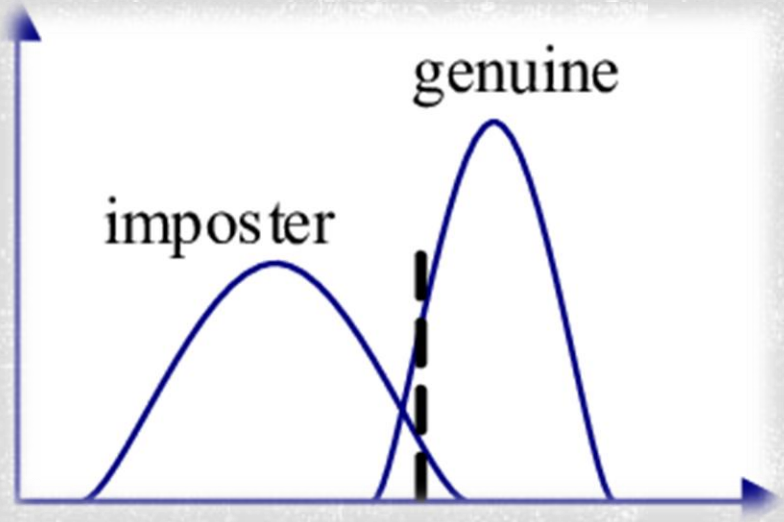
$$FMR = \int_t^1 p(s \mid H_0) ds$$

$$FAR = (1 - FTC) FMR$$

BŁĘDNE DOPASOWANIE

- **Gdzie:**

- **p(s|H0) oznacza rozkład prawdopodobieństwa wystąpienia błędu systemu polegającego na przepuszczeniu osoby nieupoważnionej, w literaturze często oznaczany jako rozkład oszusta (ang. Imposter Distribution, ID),**



BŁĘDNE NIEDOPASOWANIE

- **Błędne niedopasowanie – pojawia się kiedy system uzna za niezgodne dwie próbki pochodzące od tego samego identyfikatora biometrycznego.**

- **Błąd ten wyrażony jest za pomocą wskaźnika FNMR (ang. False Non-Match Rate – wskaźnik błędnego niedopasowania).**

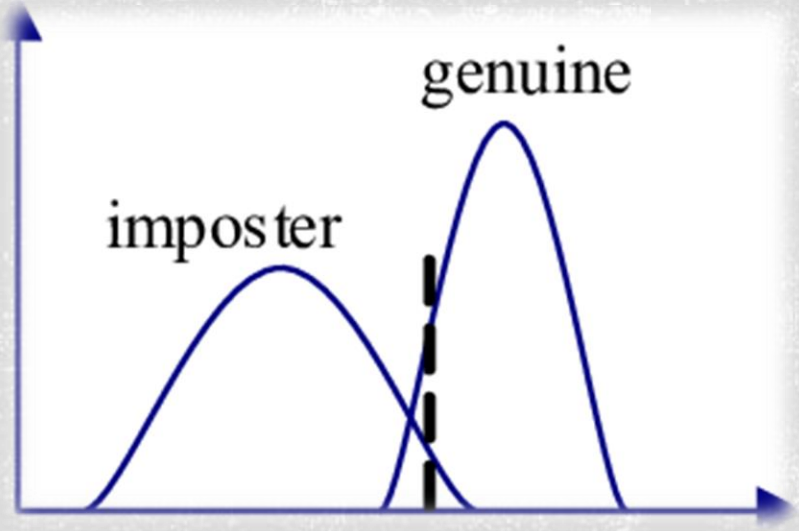
$$FNMR = \int_0^t p(s \mid H_1) ds$$

$$FRR = (1 - FTC) FNMR + FTC$$

BŁĘDNE NIEDOPASOWANIE

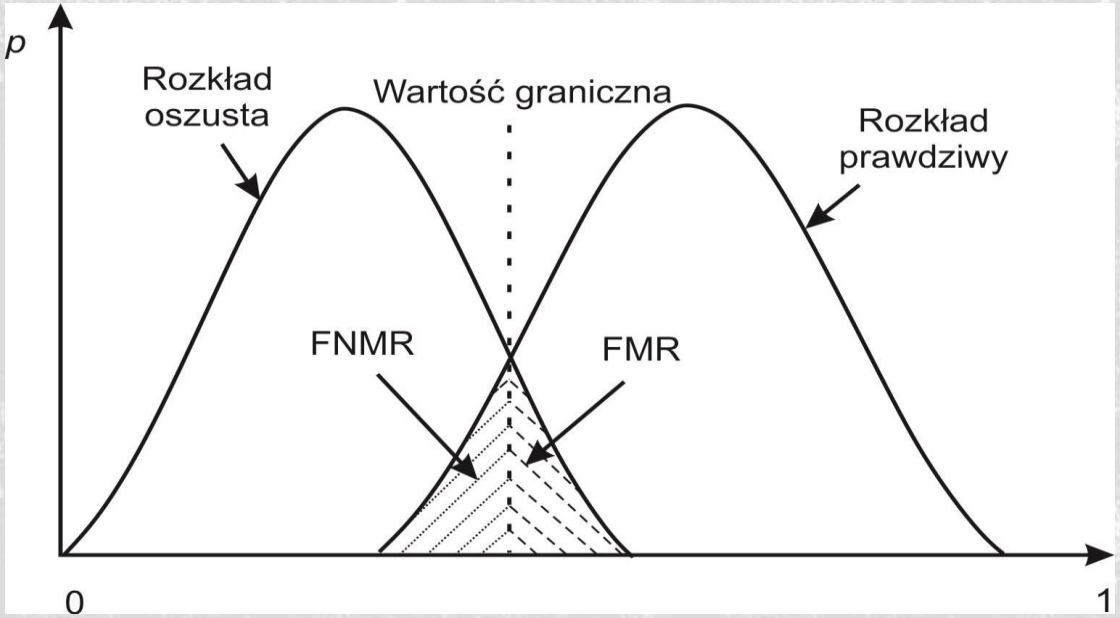
- **Gdzie:**

- **p(s|H1) oznacza rozkład prawdopodobieństwa wystąpienia systemu polegającego na nie przepuszczeniu osoby upoważnionej, w literaturze często oznaczany jako rozkład prawdziwy (ang. Genuine Distribution, GD).**



FMR I FNMR

- **Rozkłady prawdopodobieństwa FMR i FNMR są zależne od wartości granicznej, z czego wynika że zmiana granicy będzie miała wpływ na oba czynniki jednocześnie.**

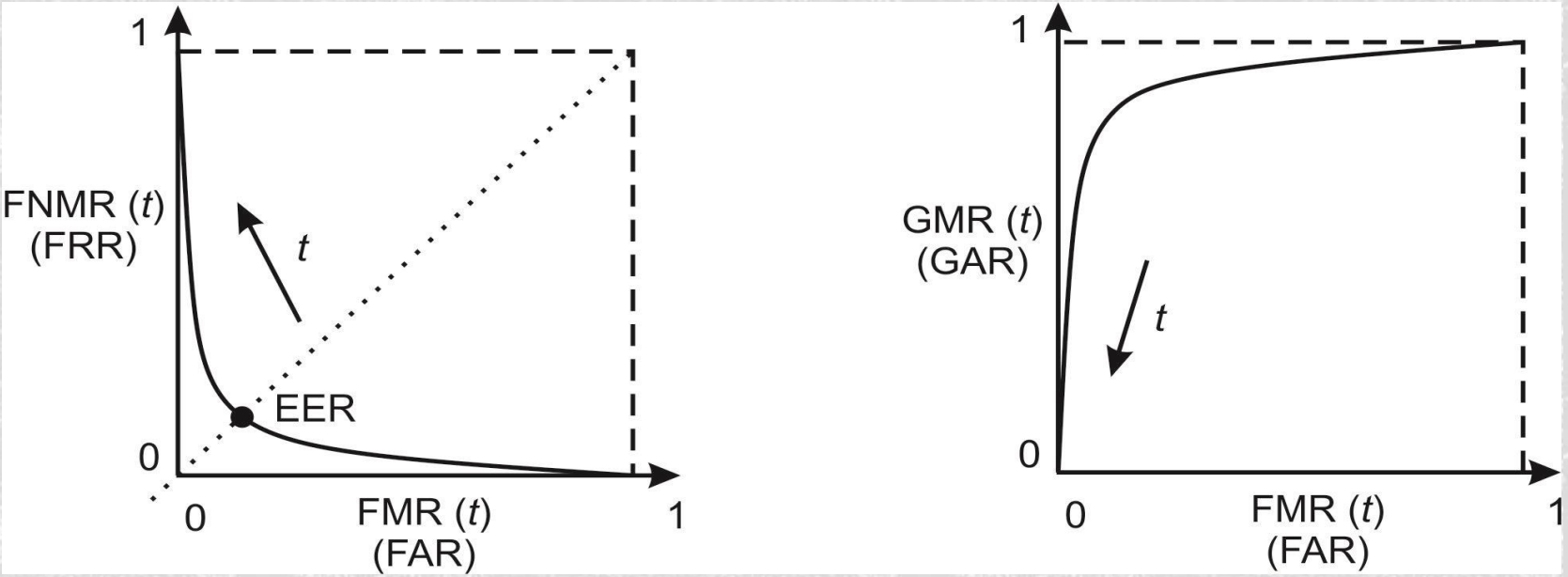


ROC I DET

- Różne poziomy FMR i FNMR mogą mieć różny wpływ na wydajność systemu biometrycznego.
- Projektant systemy zazwyczaj nie wie w jakich dokładne warunkach tworzony system będzie pracował.
- Zaleca się więc, aby wydajność mierzyć dla każdej wartości granicznej, przedstawiając ją za pomocą krzywej ROC (ang. Receiver Operating Characteristic – charakterystyka pracy odbiornika), lub krzywej DET (ang. Detection Error Tradeoff – kompromis pomiędzy wykryciem a błędem)

ROC I DET

- **Przykładowe krzywe DET i ROC dla ustalonego GMR (ang. Genuine Match Rate – prawdziwy wskaźnik dopasowania), lub GAR (ang. Genuine Accept Rate – prawdziwy wskaźnik akceptacji)**



Politechnika Częstochowska

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

Politechnika Częstochowska

KI

Dziękuję za uwagę

dr hab. inż. Mariusz Kubanek, prof. PCz
mariusz.kubanek@icis.pcz.pl
Katedra INFORMATYKI