KEMT
Department of Electronics and Multimedia Telecommunications

Táto prednáška bola realizovaná vďaka projektu KEGA 009TUKE-4/2019

Úvod do biometrických systémov bezpečnosti

MATUS PLEVA*

* TECHNICAL UNIVERSITY OF KOSICE, LETNA 9, 04120 KOSICE, SLOVAKIA

Úvod

- Definícia biometriky
- Motivácia a vznik biometrických systémov
- Typy biometrických senzorov: fyzikálne a behaviorálne (správanie)
- Porozumenie silnejším, slabším stránkam a limitom biom. systémov
- Chybovosť a vyhodnocovanie kvality biom. systémov
- Štandardy, bezpečnosť, spoľahlivosť, použiteľnosť biom. systémov
- Trendy v biom. systémoch

Definícia biometriky

- Slovo biometria pochádza z gréckych slov bio βιο- život a metrikós μετρικός - merať.
- V slovenčine používame pojem biometria na vednú oblasť a biometrika na charakteristiky živých bytostí
- Biometrický systém je technologická platforma, ktorá používa informácie o človeku na jeho identifikáciu
- Biometrika slúži na meranie a štatistická analýza unikátnych fyziologických a behaviorálnych charakteristík.

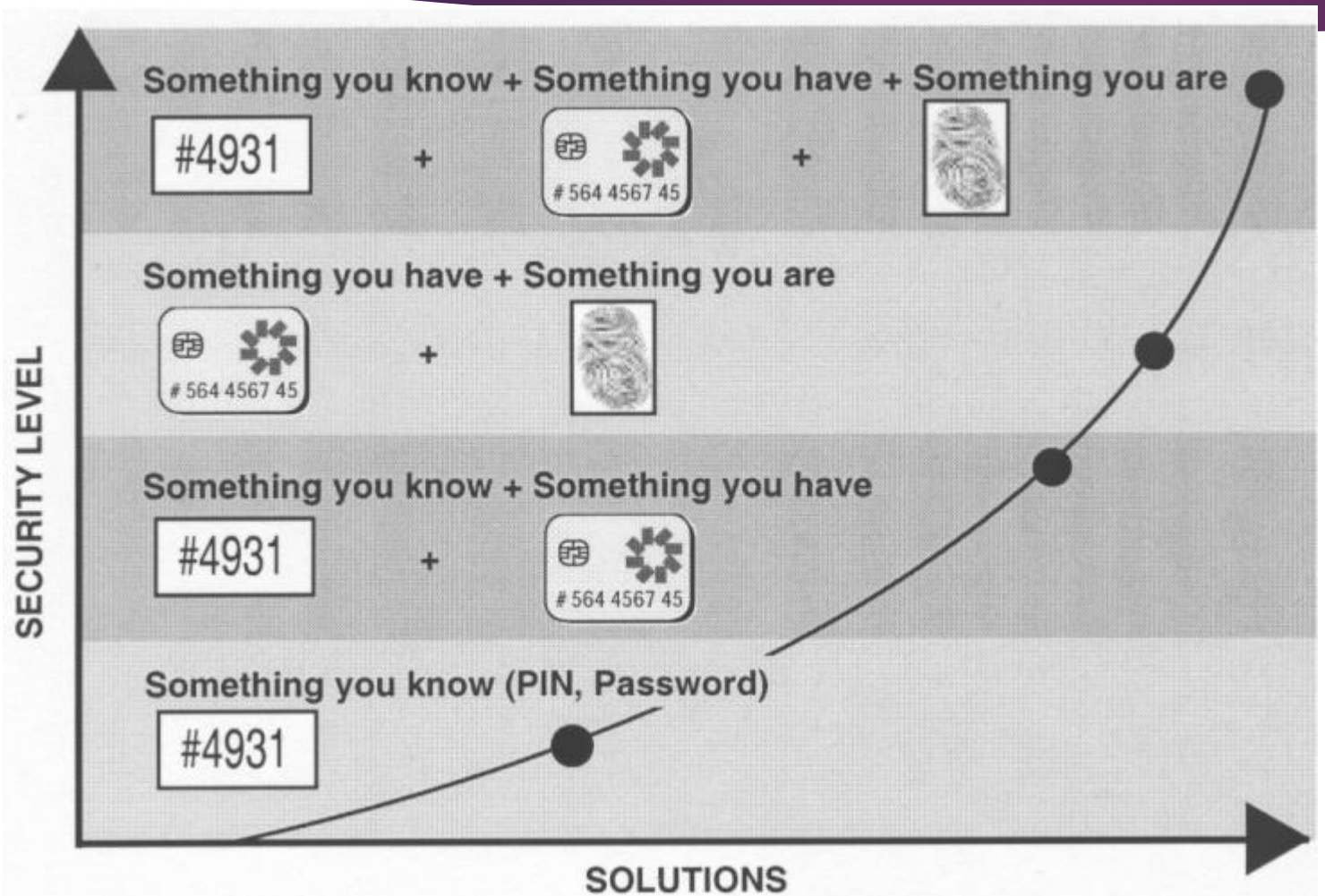
Aplikácie biometrických systémov

- bankové služby
- hraničné kontroly
- zdravotné elektronické služby
- platobné terminály/služby
- kontrola vstupu do objektu (firma, byt, garáž, telocvičňa, záujmový útvar, atď.)
- letiskové bezpečnostné služby
- kriminalistika a bezpečnostné zložky

Aplikácie biometrických systémov

- forenzné systémy
- automatizované systémy kontroly premávky (rýchlostná kontrola s fotkou)
- lotériové terminály
- vernostné systémy
- knižničné a školiace systémy
- Školy
- systémy na vzdialené preskúšavanie/testovanie (či už školské alebo certifikačné)
- mobilné telefóny a prístup k údajom v nich

Zvyšovanie zabezpečenia s využitím biometriky



CSE 190 Topics in CSE: Introduction to Biometrics with Dr. David Kriegman

ľudia sú identifikovaný na základe toho čo:

- **Majú** (ID karta, pas, rodný list, kľúče, platobná karta, atď.) - token,
- **Vedia** (heslo, PIN, meno, rodné číslo, atď.),
- **Sú** (biometrické znaky ľudského tela, teda znaky, ktoré dokážeme odmerať)

https://cseweb.ucsd.edu/classes/wi10/cse190/lec1.pdf

Biometrické znaky majú byť:

- Univerzálne (universality) - teda, každý zdravý človek by mal daný znak mať(ide hlavne o ich polohu na ľudskom tele, kde samozrejme aj to že daný znak tam nie je predstavuje dôležitú informáciu - chýbajúce tetovanie, prípadne strata končatiny či prsta),
- rozlíšiteľné/unikátne(distinctiveness) - malo by byť možné nájsť rozdiely v danom znaku/charakteristike medzi rôznymi osobami,
- trvalé/stále(permanence) - znaky by sa nemali rýchlo meniť, pričom samozrejme úrazmi a starnutím dochádza k ich zmenám,
- snímateľné(collectability) - znaky by malo byť možné relatívne jednoducho merať, snímať - senzory by mali byť dostupné a jednoducho rozšíriteľné.

Biometrický systém má byť:

- Výkonnosť/spoľahlivosť (performance) - či daný biometrický znak je relatívne rýchlo a jednoducho snímateľný, parametrizovaný a porovnaný s uloženou databázou.
- Prijateľnosť/akceptovanie(acceptability) - ako je (alebo by mohol byť) daný systém akceptovaný/prijatý používateľmi, či daný biometrický znak nie je nepríjemné a zdĺhavé zosnímať, či sa budú pri používaní cítiť komfortne a podobne.
- Neklamnosť/nespochybniteľnosť(circumvention) - systém by mal byť ťažké oklamať, či spochybniť identitu, ktorú prijal za pravú/autentickú.

Základné pojmy

- **Genuine** – pravý, známy používateľ
- **Impostor** – nepravý, neznámy používateľ, podvodník
- **Enrollment** – zaradenie do databázy, pridanie medzi známych – genuine
- **Extrakcia príznakov** (features) a trénovanie **modelu/vzoru** – extrakcia vhodných znakov zo získaných údajov a vytvorenie modelu či vzoru (template) s ktorým je možné jednoducho a rýchlo ďalšie znaky porovnávať
- **Porovnávanie** získaných znakov s jedným (*autentifikácia/verifikácia*, 1:1) alebo viacerými (*identifikácia*, 1:N) modelmi/vzormi, existuje aj N:N identifikácia – výsledkom je počet známych a neznámych identít z davu

Autentifikácia vs Identifikácia

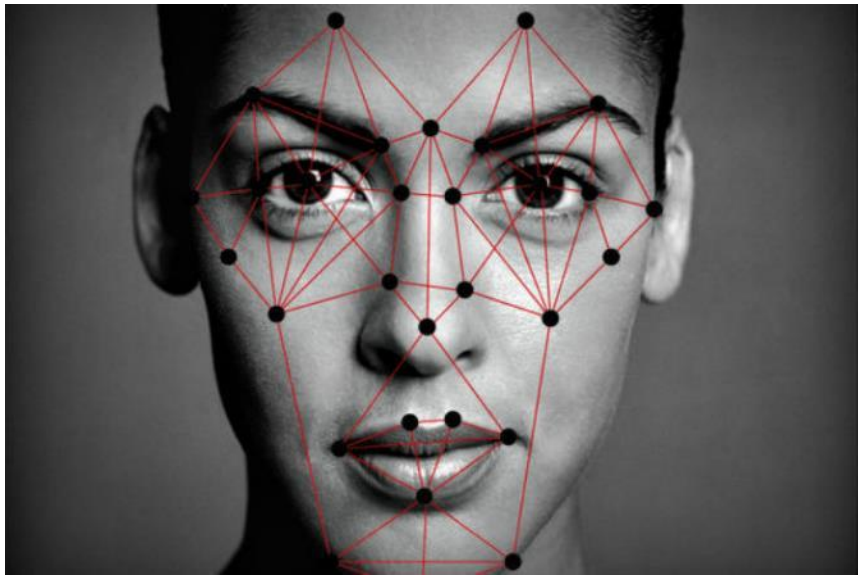
- V biometrických systémoch sa na **autentifikáciu/verifikácia** používa metóda *one2one* (1:1) teda porovnanie *proklamovanej identity s identitou a jej biometrickými znakmi z databázy*. V tomto prípade *nedochádza* k porovnaniu s modelmi/vzormi/znakmi *iných používateľov,* čo môže viditeľne *urýchliť* autentifikačný proces v rozsiahlych databázach. Autentifikácia je overenie proklamovanej identity a jej *výsledkom je binárne rozhodnutie prijatie alebo zamietnutie vstupu na základe* ***prahovej hodnoty*** *skóre/pravdepodobnosti*. Hodnotí sa pravdepodobnosť chyby – EEE: Equal Error Rate – vysvetlíme neskôr.
- **Identifikácia** - *one2many* (1:N), *porovnávaním biometrických znakov so všetkými známymi modelmi/vzormi z databázy*. Nevýhoda: zdĺhavý proces a nezaručuje autenticitu užívateľa. Vyhodnocuje najpodobnejšiu identitu s nejakou pravdepodobnosťou – systém sa hodnotí podľa presnosti (Accuracy)

Statická vs Kontinuálna autentifikácia

- ***Statická*** – overenie identity len pri vstupe do chráneného systému
- ***Kontinuálna*** – biometrická analýza beží počas celého času v chránenom systéme a keď pravdepodobnosť že nejde o pravého/genuine používateľa narastie nad určitý prah je vyzvaný na jednorázové dodatočné overenie identity. Môže byť sledovaná tvár, hlas, pohyby myšou, dynamika písania na klávesnici a iné.

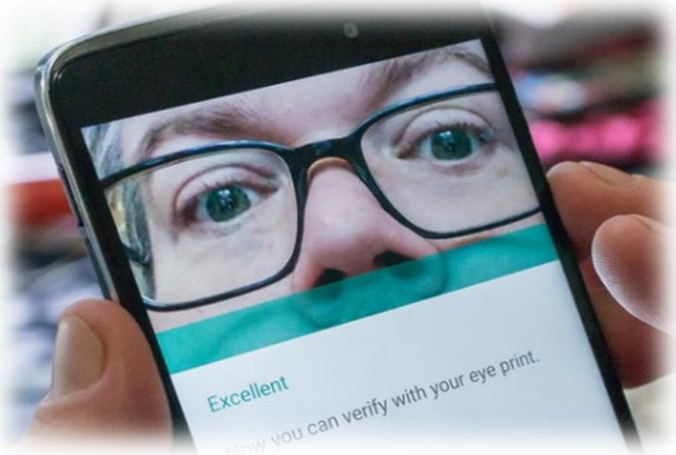
Fyziologické biometrické znaky

- *body odor - telesný pach či vôňa, bakteriálny odtlačok (forensic)*
- Tvár - fyzikálne ale aj termálne emisie
- *Eye* features as *iris* or *retina* – oko, dúhovka alebo očné pozadie (rohovka)
- Tvar ucha, prstov, nohy, odltačok zubov, RTG
- *Odtlačok prsta (Fingerprints) a odtlačok dlane (Palmprints) – štruktúra kože na prstoch, dlani, nohe (deti) – senzor existuje optický, kapacitný, ultrazvukový, tlakový, termálny, atď.*
- *Palm/Finger vein* – štruktúrna krvného riečišťa pod kožou – infra
- *Hand geometry* – geometria ruky
- *Póry na koži (Skin pores) a žily na zápästí/ruke (wrist/hand veins)*
- *DNA*
- *EKG či EEG(pomocou smart wearables – nositeľné inteligentné zariadenia)*
  - zmena parametrov starnutím - vek, výška, hlas, hmotnosť, veľkosť chodidla, špeciálne znaky (tetovania, jazvy, atď.)



Biological biometric sensors

- *Body odor – stress related*
- *Facial* & thermal emissions – camera (built-in) & thermo camera (expensive)
- *Eye* features as *iris* or *retina* – cell phone built in camera
- *Fingerprints & Palmprints – external sensors for higher EER (Equal Error Rate) – not accurate built in portable scanners,* (price for sensor on the picture ~$130)



Biological biometric sensors

- *Palm vein* - the composition of vein in the palm of the right hand is a very accurate biometric feature (price ~ $400)
- *Hand geometry* - the geometry of the hand and fingers is the most widespread way of simple authentication when checking entry to exclusive areas, usually after entering your access code (~$2,000)
- *Skin pores & wrist/hand veins* - these new technologies are just in development and the sensors are not off-the-shelf

Behaviorálne biometrické znaky

- *Handwritten signature* – electronic pen with a special pad – ručný podpis (statický, dynamický, dyn. + tlak)
- pupillary light reflex (PLR) – how the pupil change in different lightning conditions – pupilárny/zrenicový reflex na svetlo
- *Keystroke dynamics – klávesová dynamika – snímanie časov z klávesnice*, zvuk, EEG náramok
- *Voiceprint – hlasový odtlačok*
- *Gait* – chôdza
- *Gesture – gestá, Lip motion – pohyby pier*
- *Mouse movements – pohyby myšou*
- *Používanie mobilného telefónu: touch,* accelerometer, gyroscope, magnetometer, proximity, ambient lighting, gravity, pressure sensor, location, user activity, call data, SMS, app usage, browser history, phone status, secondary camera, stylometry (txt analysis) (*Eglitis, T., Guest, R. and Deravi, F., 2020. Data Behind Mobile Behavioural Biometrics–a Survey. IET Biometrics*.)
- *Iné?*

Error rates in biometric systems – binary classificators for verification

Predicted/Actual class	Yes (Genuine)	No (Impostor)
Yes	TP – True Positive	FP – False Positive
No	FN – False Negative	TN – True Negative

False acceptance **rate** (FAR; Miss probability) Falošné prijatie/vpustenie=

$$\frac{FP}{TP + FP}$$

False rejection rate (FRR; False alarm probability) =

$$\frac{FN}{TN + FN}$$

https://beso.tistory.com/5

- **FAR** (False acceptance rate) - percento falošne prijatých identít (do systému bol vpustený používateľ s falošnou identitou - impostor/podvodník), niekedy sa označuje aj ako False Match Rate - FMR či False Positive Rate - FPR (pozri obrázok 2.1).

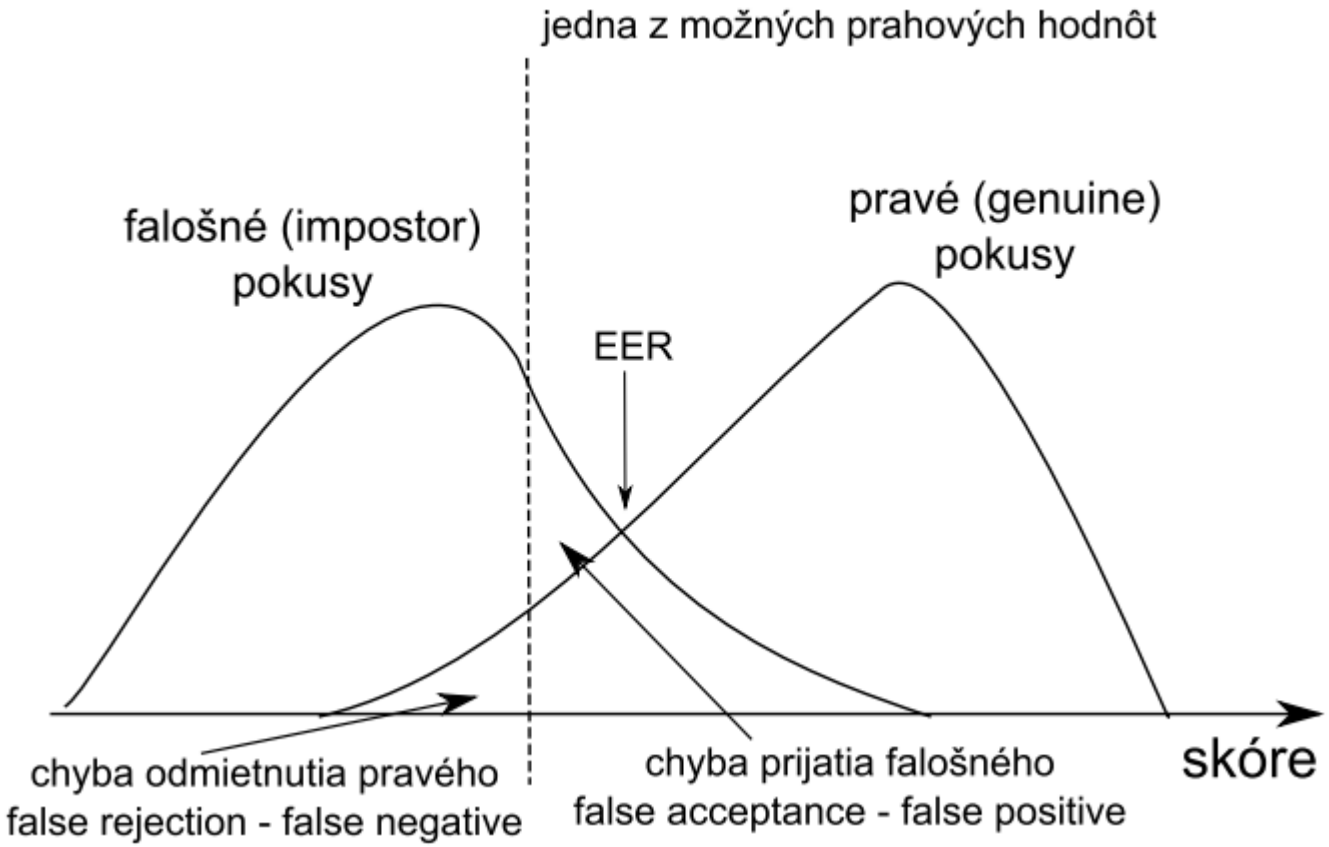
- **FRR** (False rejection rate) - percento nesprávne zamietnutých identít (používateľovi s pravou identitou (genuine) bol prístup zamietnutý), niekedy sa označuje aj ako False Non-Match Rate - FNMR či False Negative Rate - FNR.

- FTD (Failure to Detect) + FTC (Failure to Capture) [6] - percento chybovosti pri snahe detegovať (FTD) biometrický objekt (napríklad tvár, prst a podobne) alebo spracovať zo získanej snímky/záznamu (sample) vhodné parametre (FTC) kvôli jej zlej kvalite, expozícii, šumu, špine a podobne.

- FTP (Failure to Process) + FTE (Failure to Enroll rate) - percento chybovosti pri zaradení do databázy - môže byť problém so získaním dát zo senzora (FTC), alebo je napríklad daný biometrický znak pri zosnímaní poškodený (môže byť aj špinou na prstoch, zakrytou tvárou, atď.), alebo nie je dostatok vzoriek na zaradenie do databázy (FTP), väčšinou na zvýšenie presnosti systému požadujeme niekoľko úspešne získaných a kvalitných vzoriek.

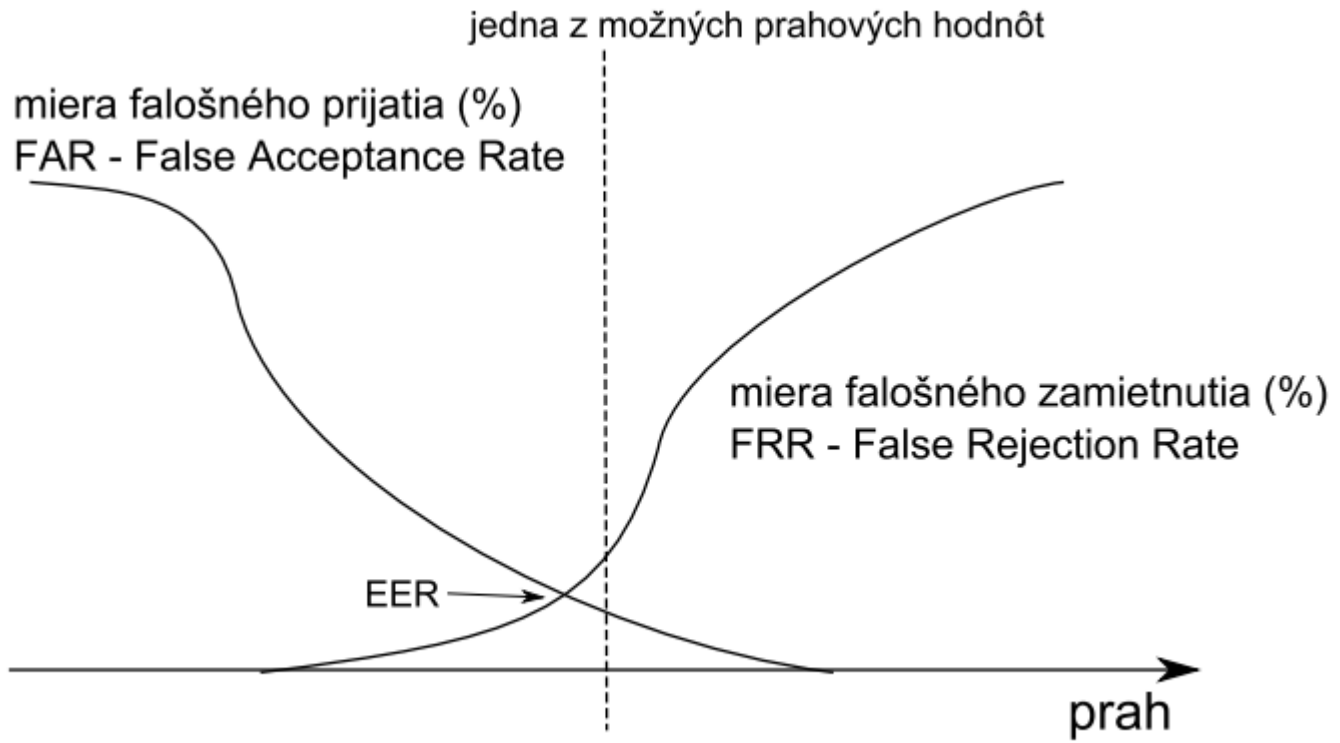
- FTA (Failure to Acquire rate) - percento chybovosti prí získaní dát v procese verifikácii/identifikácie - opäť môže ísť o problém pri získavaní dát (senzor, biometrický znak, kvalita, atď.) prípadne systémová chyba algoritmu či modelu v databáze získaného napríklad v iných podmienkach (svetelných, akustických, vlhkosť, hmla, atď.).

Histogram výskytu skóre pri verifikácii

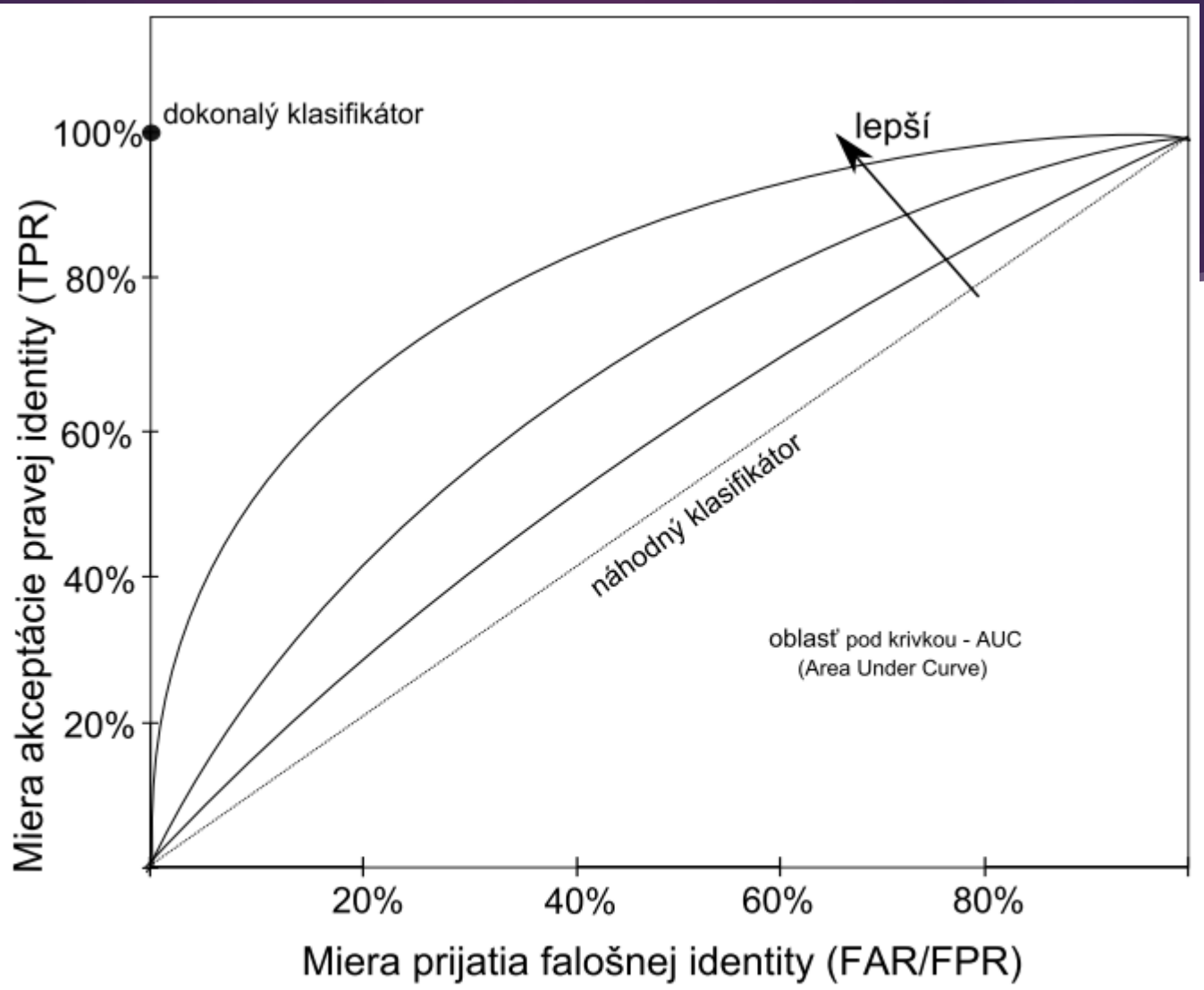


EER

Aby sme dokázali porovnať rôzne autentifikačné systémy (1:1), bez ohľadu na to na akú bezpečnosť/prah je systém pri akceptácii identity nastavený, bol zvolený parameter EER (Equal Error Rate) teda percento chybovosti systému v bode kedy FRR a FAR sú zhodné, či inak povedané chybovosť systému v bode kedy pravdepodobnosť vpustenia falošného (impostor) používateľa - podvodníka je rovnaká ako pravdepodobnosť nevpustenia používateľa s pravou identitou (genuine). Samozrejme systém pri svojom chode môže mať inak nastavenú prahovú hodnotu a neznamená to že pri systéme s EER 5% má používateľ automaticky očakávať že ho systém s 5% pravdepodobnosťou nevpustí. Administrátor môže prah na akceptovanie identity nastaviť tak, že pravdepodobnosť nevpustenia bude len 1% ale samozrejme pravdepodobnosť vpustenia cudzej/nepravej identity sa zvýši na povedzme 8 či 15%.

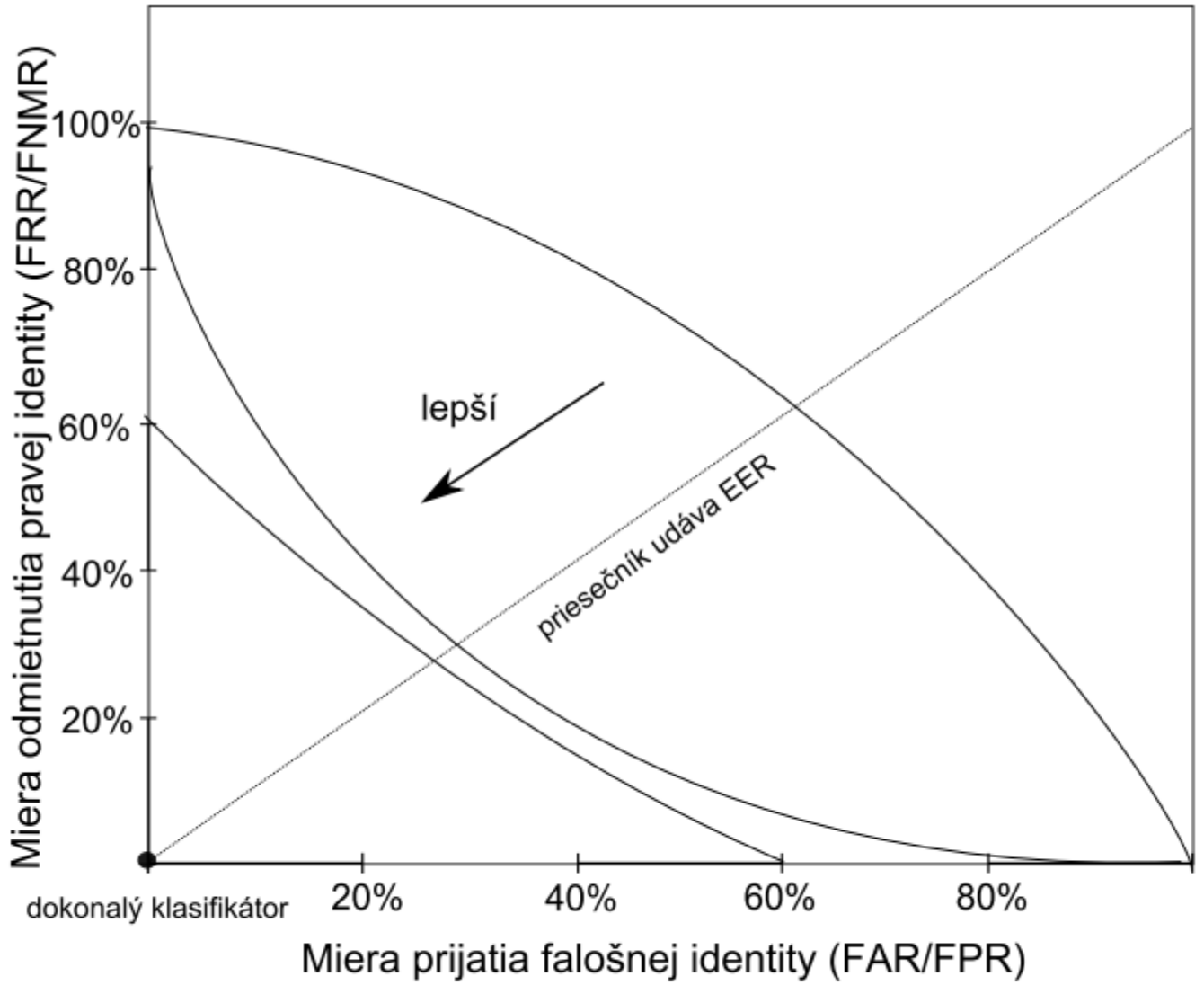

jedna z možných prahových hodnôt
miera falošného prijatia (%)
FAR - False Acceptance Rate
miera falošného zamietnutia (%)
FRR - False Rejection Rate
EER
prah

ROC



Obr. 2.3 ROC krivka - operačná charakteristika binárneho klasifikátora

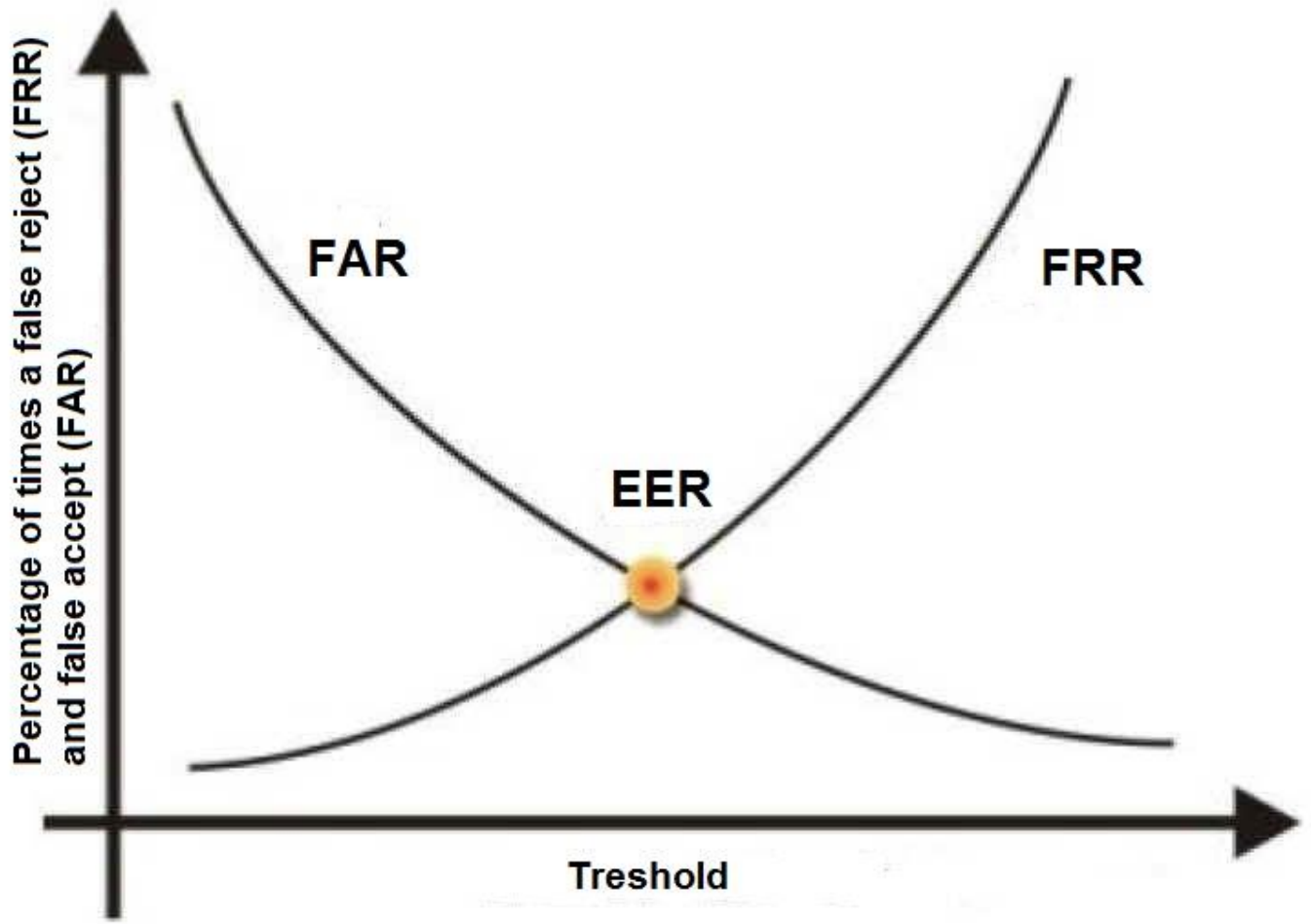
DET



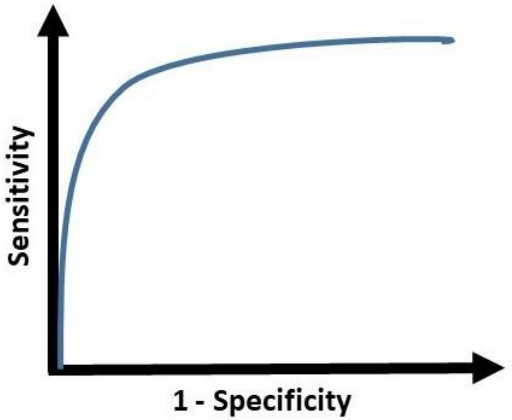
Obr. 2.4 DET krivka - kompromis detekčnej chyby

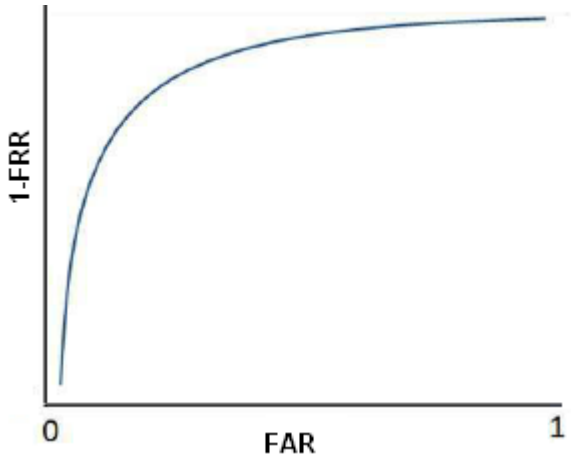
Error rates in biometric systems

- For authentication purposes: FRR, FAR, EER
  - False rejection & False acceptance rate depends on threshold, so for threshold when FAR=FRR the error rate is called Equal Error Rate
- For identification purposes: Accuracy = percentage of correctly recognized person

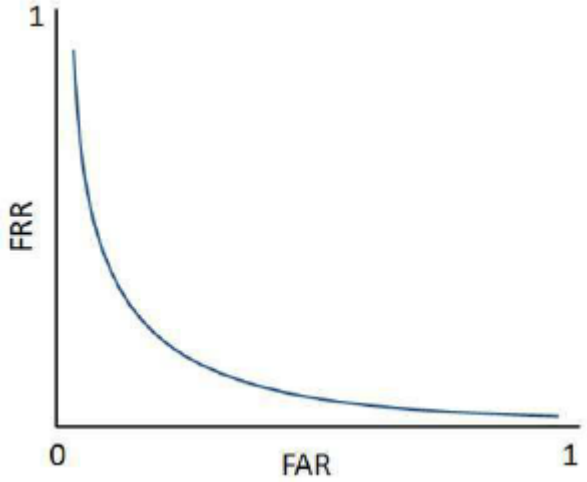


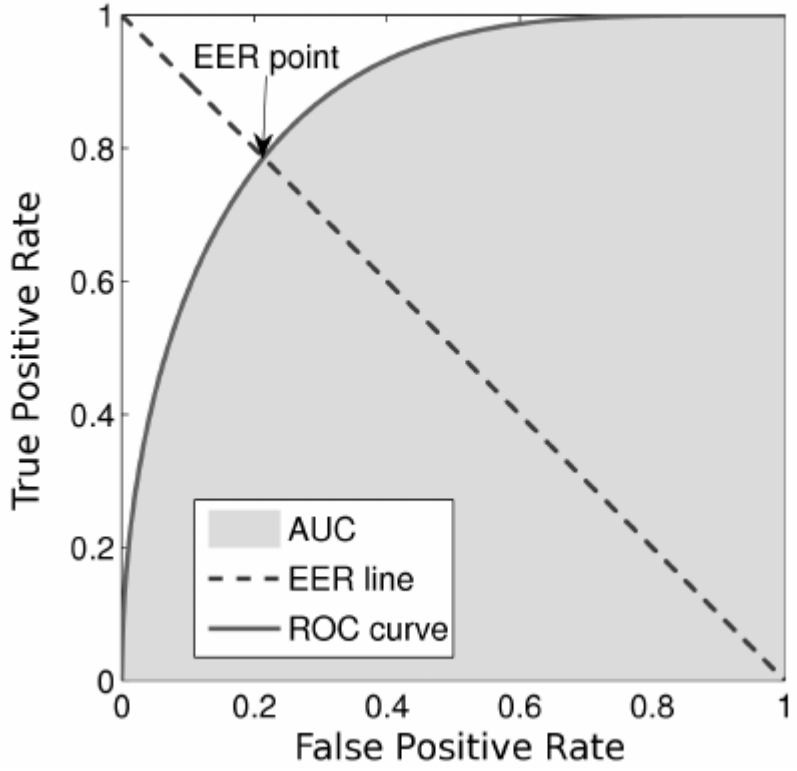
Error rates in biometric systems

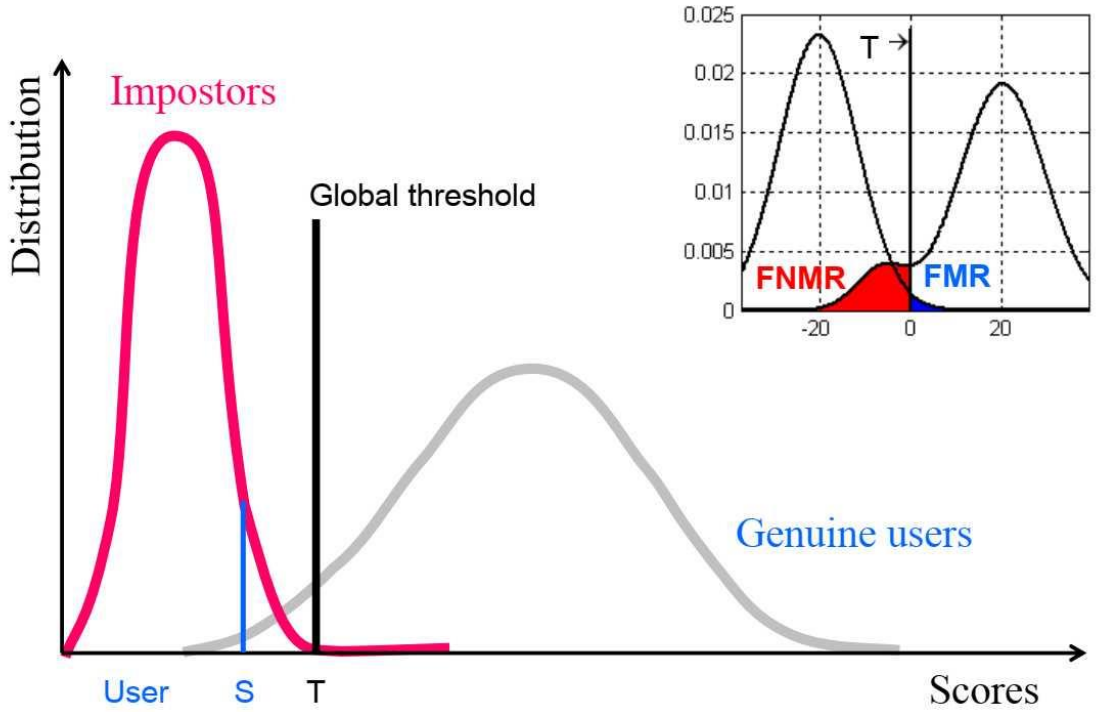




- Receiver operating characteristics (ROC) curves provide critical performance insights for the evaluation of an authentication algorithm.







Daniel Novák: Biometrics. Introduction.
Slides from
https://cw.fel.cvut.cz/b191/courses/a6m33bio/start

Iné biometrické techniky

- *Soft biometrics* – Kombinácia viacerých rôznych anatomických či behaviorálnych charakteristík od jedného používateľa môže zvýšiť pravdepodobnosť, že sa zhoduje iba s jedným známym užívateľom. Ľahko zistiteľné charakteristiky (napr. aj zo zdravotnej dokumentácie) sú zvyčajne váha, výška, vek, farba očí, farba pleti, tetovanie, prítomnosť fúzov / fúzov / make-up / okuliare, etnická príslušnosť, tvary tváre, nezvyčajné znaky, oblečenie atď.
- *Multimodal biometrics* – Multimodálny systém využíva viacero senzorov / algoritmov / vzoriek / jednotiek (pravé a ľavé oko, viac prstov, ...) / čŕt, je potrebné riešiť fúziu rôznych výstupných pravdepodobností
- *Biometrics in the Wild* – Dáta získané vonku z veľkých vzdialeností, senzorov s nízkym rozlíšením alebo bez spolupráce subjektu znižujú schopnosť identifikovať osobu

Nedostatky biometrických systémov

- Sú drahšie ako použitie tokenov (heslo, ID karta, ...).
- Pri problémoch s nasnímaním biometrických dát systém nie je schopný vyhodnotiť autenticitu.
- Databázy s biometrickými dátami môžu byť ukradnuté.
- Nie sú bezchybné – kto je zodpovedný za chybu?
- Pri chorobe alebo zranení je množstvo biometrických znakov dočasne alebo trvalo poškodených.

Spoľahlivosť, bezpečnosť, štandardizácia

- Ako môžeme zdieľať získané dáta z rôznych senzorov s rôznymi databázami a systémami? Existuje štandardizácia?
- Ako sú biometrické dáta ukladané a prenášané? Je môžné ich ukradnúť a zneužiť? – šifrovanie, cancelable/revocable biometrics, blockchain?
- Ako zabrániť zneužitiu biometrických dát? spoofing -> liveness detection
- Ako je biometrický systém odolný voči hackerom?

Thanks for your attention

Questions?

This work was realized thanks to KEGA 009TUKE-4/2019 project

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY