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

Overview of the Current Biometrics Technologies

MATUS PLEVA[*], JOZEF JUHÁR[*], PATRICK BOURS[**]

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

[**] NORWEGIAN INFORMATION SECURITY LABORATORY (NISLAB), NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY, GJØVIK, NORWAY

Introduction

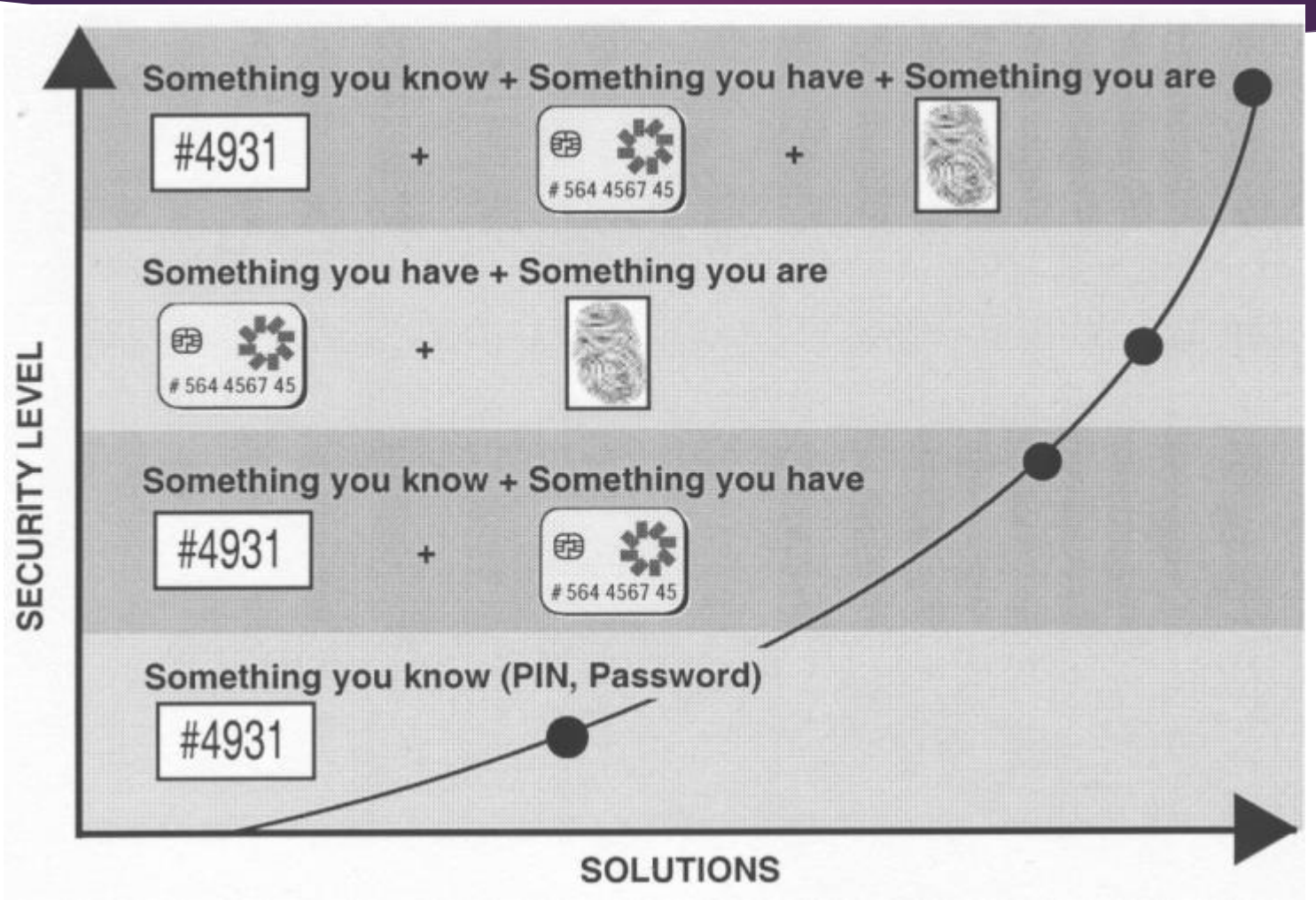
- Definition of biometric technologies
- Origin and evolution of biometrics
- The need for biometric systems
- Types of biometrics including physical and behavioural modalities
- Understanding biometric, strengths, weaknesses and limitations
- Features of biometrics
- Error rates
- Biometric standards, privacy, spoofing and system security
- Future directions and development of emerging technologies.

Definition of biometric technologies

- A biometric system is a *technological system that uses information about a person (or other biological organism) to identify that person*.
- Biometric systems rely on specific data about *unique biological traits* in order to work effectively.
- A biometric system will involve *running data through algorithms* for a particular result, usually related to a positive identification of a user or other individual.
- Biometrics is the *measurement and statistical analysis of people's unique physical and behavioral characteristics*.
- The term *biometrics* is derived from the Greek words *bio* meaning *life* and *metric* meaning *to measure*.

- Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry.
- Some biometric methods, such as measuring a person's gait, *can operate with no direct contact with the person* being authenticated.
- Components of biometric devices include:
  - A *reader or scanning device* to record the biometric factor being authenticated.
  - *Software* to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data.
  - A *database* to securely store biometric data for comparison.

Increasing security with biometrics



Static vs Continuous authentication

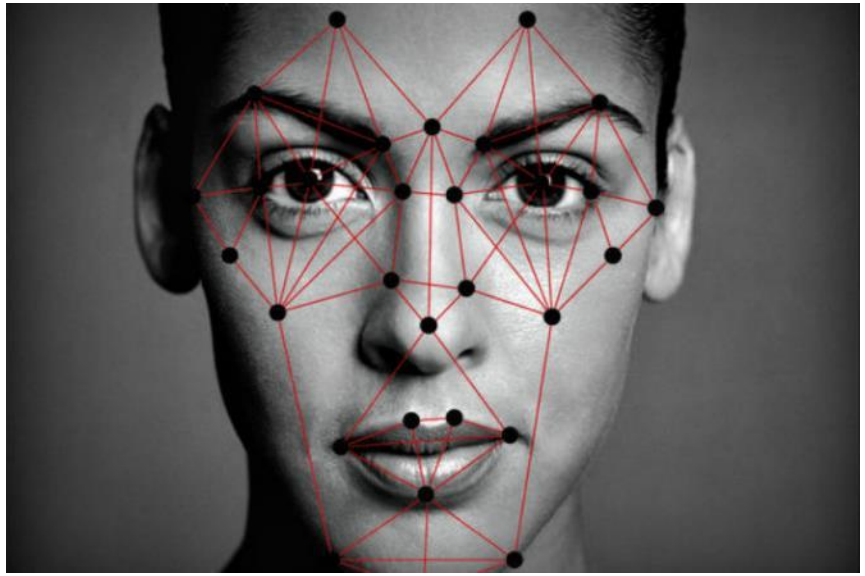
- ***Static*** authentication – *authentication ONLY during the login process* as additional feature or in repeated checking intervals
- ***Continuous*** authentication – the biometric analysis is *continuously running during the assessment session*, and when the trust in the genuineness of the current user falls below defined threshold, the *system alerts the user that additional authentication is needed* to prove that this user is genuine and usually one of the highly reliable static authentication methods are used.

Steps in user authentication

- **Enrollment** – the acquisition of biometric features is realized in a defined amount of time *during the* course management system *user registration*; the result of the enrollment process is a template or a model of the user and stored in the enrollment database.
- **Identification** or Recognition – the user is compared with all users that the system knows;
- **Authentication** – The user features are *only compared with his/her own models or templates*. The defined threshold for confirmation of the identity is the *most important part of the system*.

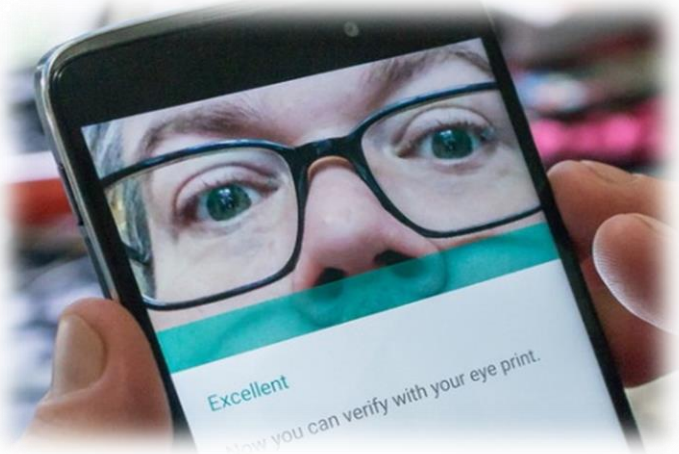
Biological biometric features

- *Body odor* – chemical composition and metabolism features of the human
- *Facial* features and thermal emissions , *ear* shape
- *Eye* features as *iris* or *retina*
- *Fingerprints & Palmprints*
- Finger geometry (the size and position of fingers).
- *Palm vein*
- *Hand geometry*
- *Skin pores & wrist/hand veins*
- *DNA* matching



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

Behavioral biometrics

- *Handwritten signature* – electronic pen with a special pad
- *Keystrokes* – the *timing* information gathered from the keyboard driver or the *audio* capture of the *keyboard sounds* can be used to analyze the user behavior while typing
- *Voiceprint* – speaker authentication using voice (noise, stressed voice)
- *Gait* – the motion of the human body while walking (distance camera)
- *Gesture* – the gestures of the head/face and hands are usually captured by the camera (could be depth- or 3D- camera for better results)
- *Mouse movements* – the movements of the wired or wireless mouse

Other biometric techniques

- *Soft biometrics – Combination of more characteristics* from one user could increase the probability that he matches only one template. The characteristics that are *easy to read* are usually the user's *weight, height, age, eye color, skin color, tattoos, presence of beard/moustache/make-up/glasses, ethnicity, facial shapes, marks, clothes*, etc.
- *Multimodal biometrics* – A multimodal system contains more sensors and the different types of biometric features
- *Biometrics in the Wild* – Data acquired outdoors from large distances, low resolution sensors or without cooperation of the subject decrease the ability to identify a person

Benefits of biometric systems

- Hard to fake or steal, unlike passwords.
- Ease of use and convenience.
- Change little over a user's life.
- Are non-transferrable.
- Templates take up less storage.

Weaknesses of biometric systems

- It is costly to get a biometric system up and running.
- If the system fails to capture all of the biometric data, it can lead to failure in identifying a user.
- Databases holding biometric data can still be hacked.
- Errors such as false rejects and false accepts can still happen.
- If a user gets injured, then a biometric authentication system may not work (for example user burns their hand, then a fingerprint scanner may not be able to identify them).

Biometric standards, privacy, spoofing and system security

- How we can exchange data, captures and models between biometric systems? – standardization
- Are the stored biometric information private and nobody can steel and misuse?
- Can somebody misuse my biometric features (face, fingerprint, …)? – spoofing -> liveness detection
- Is the biometric system secure against attacker?

Common biometric usage

- Law enforcement - In systems for criminal IDs such as fingerprint or palm print authentication systems.
- Border control - In systems for electronic passports which stores fingerprint data, or in facial recognition systems.
- Healthcare - In systems such as national identity cards for ID and health insurance programs which may use fingerprints for identification.

Error rates in biometric systems

Predicted/Actual class	Yes	No
Yes	TP – True Positive	FP – False Positive
No	FN – False Negative	TN – True Negative

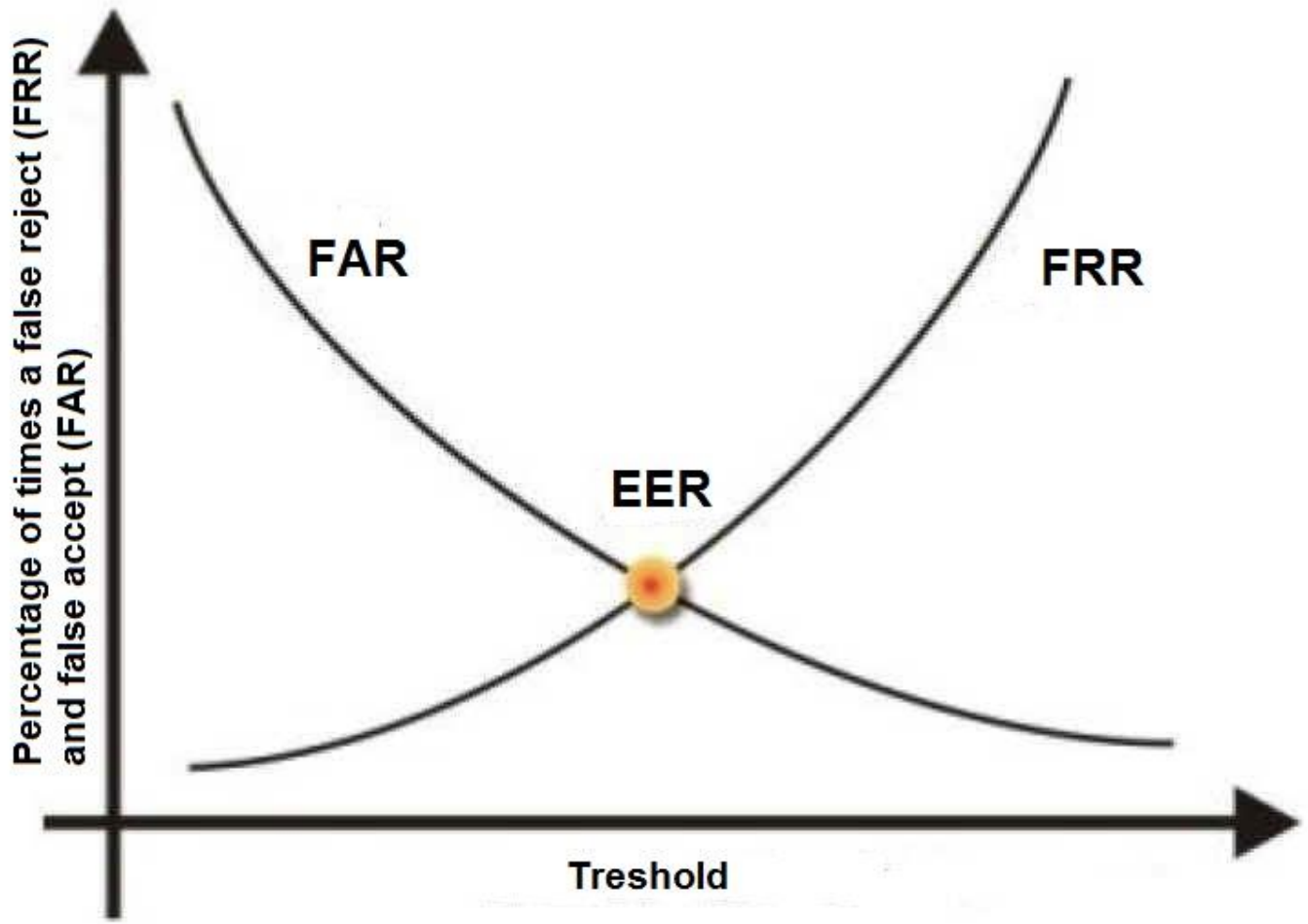
False acceptance **rate** (FAR; Miss probability) = $\frac{FP}{TP + FP}$

False rejection rate (FRR; False alarm probability) = $\frac{FN}{TN + FN}$

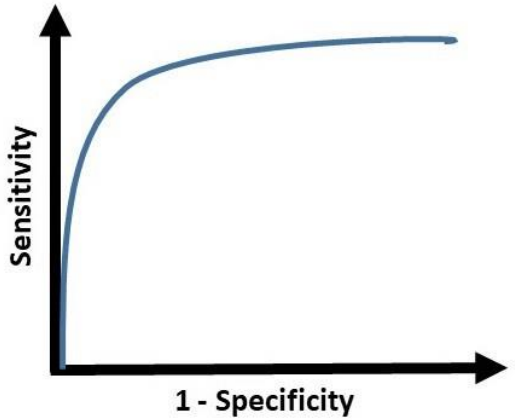
https://beso.tistory.com/5

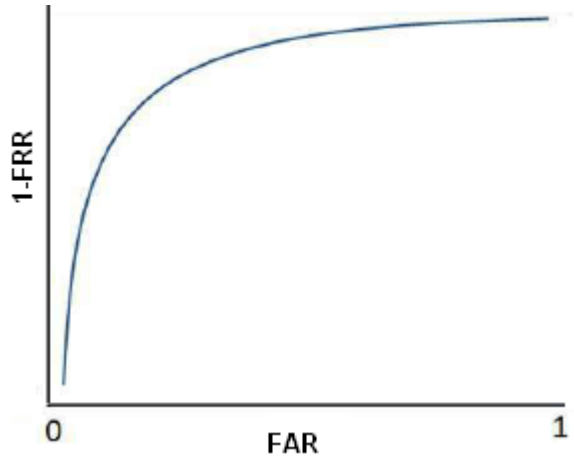
Error rates in biometric systems

- 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

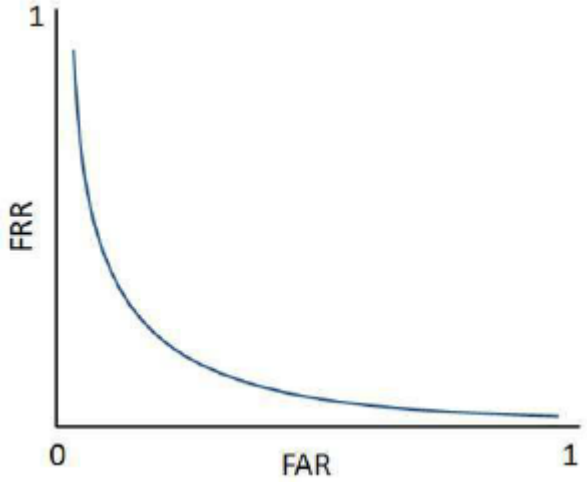


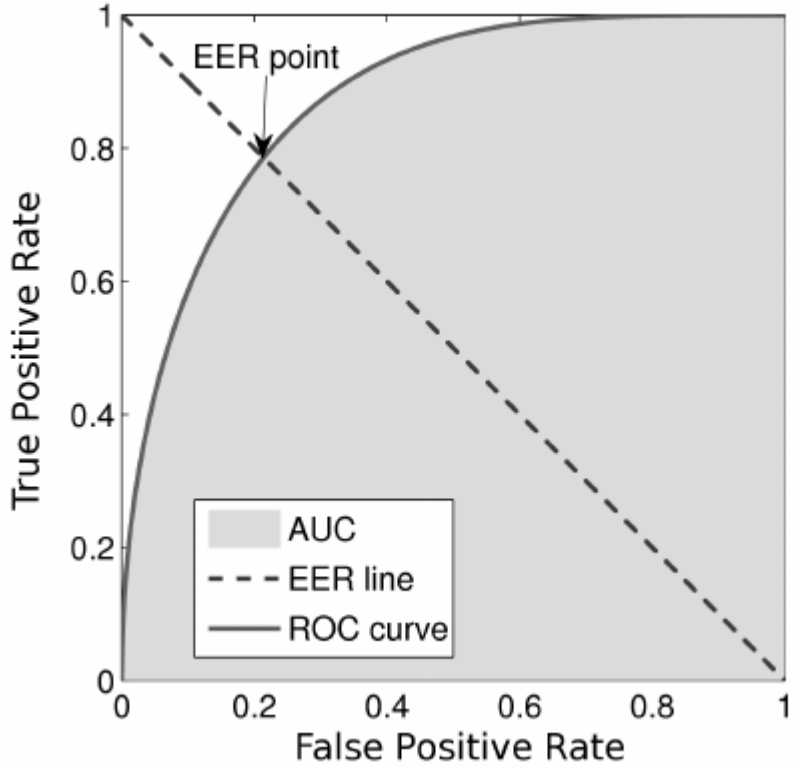
Error rates in biometric systems





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





ASSESSMENT IN E-LEARNING PLATFORMS

- in controlled environment where some authority
- "Territorial center" which provides the identity checks
- biometric solutions bring significant cost caves if no special devices are needed
- Our proposal is to use the *keystroke* and *mouse* dynamics

Proposed solution of our biometric project

- Collaboration between TUKE and Gjøvik started thanks to IWBF 2015 workshop organized by COST IC1106 "Integrating Biometrics and Forensics for the Digital Age" project
- The Gjøvik NISLab provides a keystroke dynamics database captured on their university with *timing and audio* data gathered from keyboard and webcam's microphone
- Database: 50 users with 100 captures for each (in 4 sessions – 25 typings each), Word typed is "password", "Fixed" setup, "No" background noise
- NISLab continues the research including *mouse* movements analysis

Proposed solution

- **Static:**
  Type of authentication: a static password

- **Audio:**
  We listen to the typing on the keyboard

- **Keystroke Dynamics (KD):**
  We consider not only the "value" of the password, but also the typing rhythm

Results of proposed solution

- *timing* analysis of static keystroke dynamics analysis brings 11.7% EER (Equal Error Rate)
- *audio* analysis for the same database achieved 99.33% identification accuracy but only 19.1% EER for authentication
- *audio* analysis EER was decreased to 9.4% by using *calibration setup*
- final decrease to about 4.50% EER could be achieved by using of timing and audio analysis *fusion*
- *combining the mouse and keystroke dynamics* and using the unique *Pairwise User Coupling* (PUC) the 62.2% accuracy of closed-set *continuous identification experiment* was achieved after average of 470 actions (keyboard press/release or mouse movement)

Conclusions

- using *keystroke* and *mouse* analysis is *one of the best* choices for *low-cost authentication* improvement for assessment in current e-learning systems
- *keystroke* timing and audio analysis could be used for *static authentication* during the assessment starting process
- *mouse and keystroke continuous analysis* is effective when detecting the change in the end-user behavior

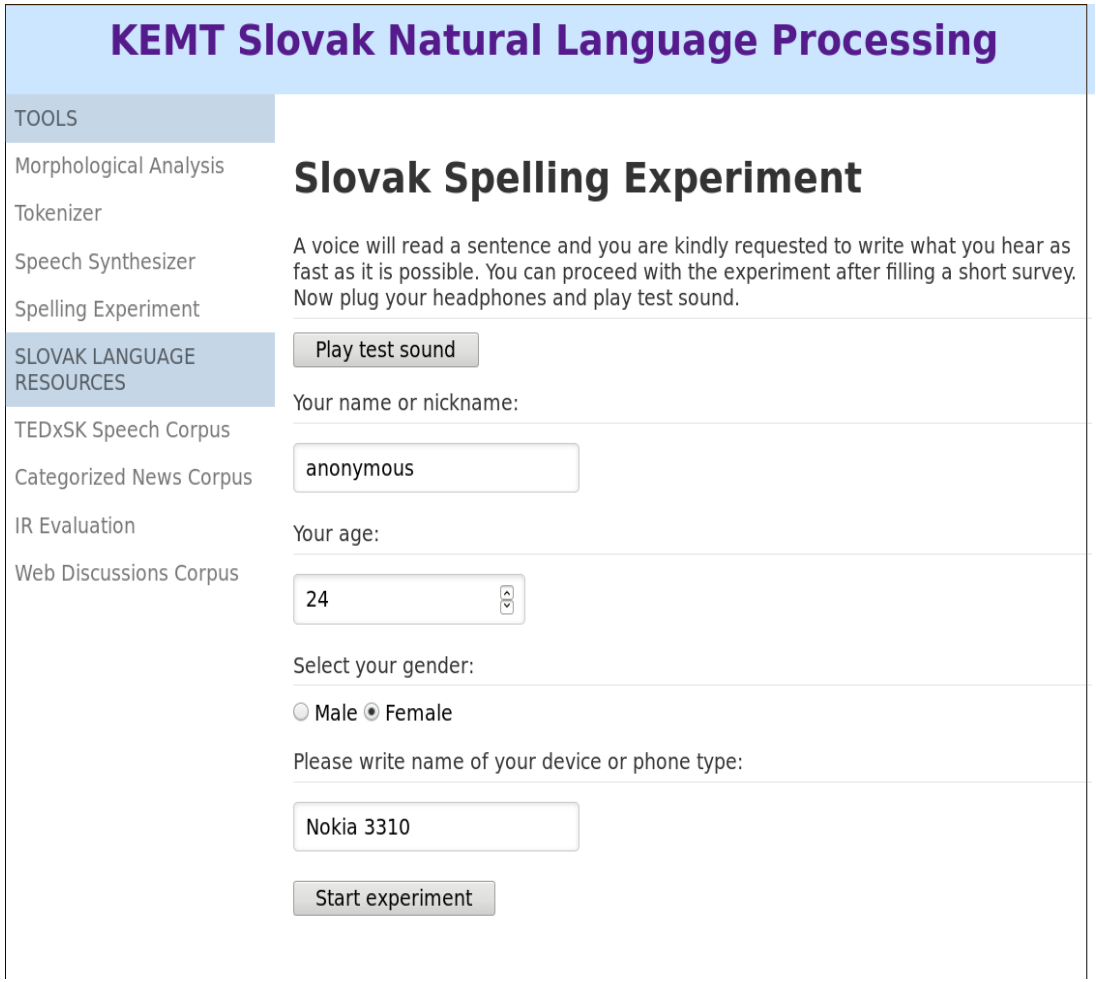
Future work

Database of Mobile Device Typing

- number and type of spelling errors depends on dimension and type of the virtual keyboard
- dynamics of typing, spelling errors and corrections is specific to a person and can be used as *authentication tool*

The sentence is read by an artificial voice to mitigate effect of visual feedback.

Already 4300 sentences by 83 participants. 818 sentences read by artificial Slovak voice.



References:

https://searchsecurity.techtarget.com/definition/biometrics

- A. Lagorio, M. Tistarelli, M. Cadoni, C. Fookes, and S. Sridharan. "Liveness detection based on 3D face shape analysis." In proceedings of: *Biometrics and Forensics (IWBF), 2013 International Workshop on*, Lisbon, Portugal, IEEE, 4-5 April 2013, pp. 1-4.
- R. Haraksim, A. Anthonioz, C. Champod, M. Olsen, J. Ellingsgaard, and B. Christophe, "Altered fingerprint detection–algorithm performance evaluation". In 2016 4th *International Conference on Biometrics and Forensics (IWBF)*, March 3-4, Limassol, Cyprus, IEEE, 2016, pp. 1-6.
- P. Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation". *Information Security Technical Report*, 17(1), Elsevier, 2012, pp.36-43.
- D.D. Zhang, *Automated biometrics: Technologies and systems.* Vol. 7. Springer Science & Business Media, 2013.
- A. Dantcheva, C. Velardo, A. D'Angelo, and J.L. Dugelay, "Bag of soft biometrics for person identification". *Multimedia Tools and Applications*, vol. 51 (2), Springer, 2011, pp.739-777.

Thanks for your attention

Questions?

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

APVV

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY