A Data Driven In-Air-Handwriting Biometric Authentication System

Duo Lu, Kai Xu, Dijiang Huang

School of Computing, Informatics, and Decision Systems,
Arizona State University

{duolu, kaixu, dijiang.huang}@asu.edu

ASU IRA A. FULTON SCHOOLS OF engineering

school of computing, informatics, & decision systems engineering

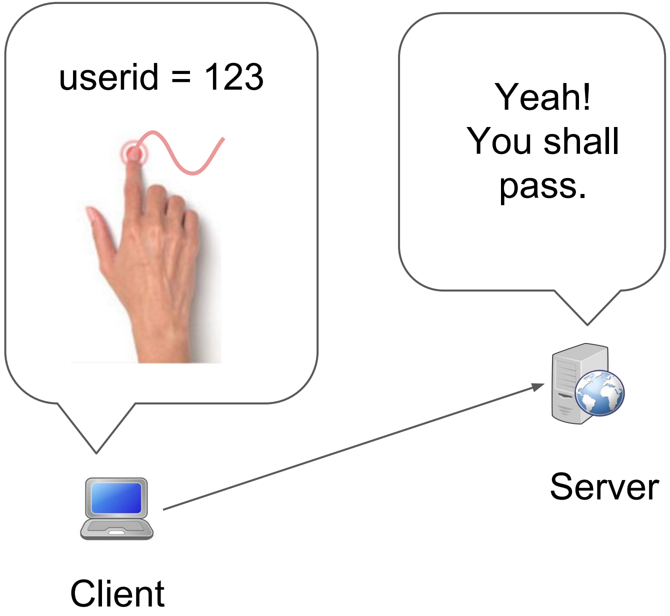
Arizona State University SNAC Secure Networking And Computing

Secure Networking And Computing Research Group

In-Air-Handwriting

- More like password than fingerprint or face
  - Changeable and revocable
  - Preserving privacy
  - Large password space,

    i.e. arbitrary strokes vs. characters
- Technical Challenges:
  - Hand movement tracking is difficult
  - Tolerating minor variations of writing
- Application Scenarios:
  - Virtual Reality applications
  - Wearable computing platforms



Objective

Verify whether you are the owner of the account that you claim to possess,

like a password:

- instead of whether you are the person that you claim to be,
- without linking the account to the person (i.e., one person multiple accounts)
- by comparing the hand motion signal with the template,

like a biometric:

- while prevent the user to give the passcode to someone else,
- and prevent spoofer (even with the leakage of the passcode content)

System Model

Template (T, C)

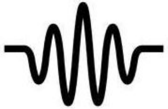
Device → Preprocess & Alignment → Feature Extraction → Decision Making

In-Air-Handwriting

passcode

Raw signal

R



Smoothed and aligned signal

S

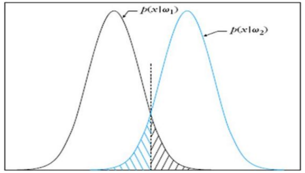
$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Feature Matrix

TD: temporal distance

SS: statistical similarity

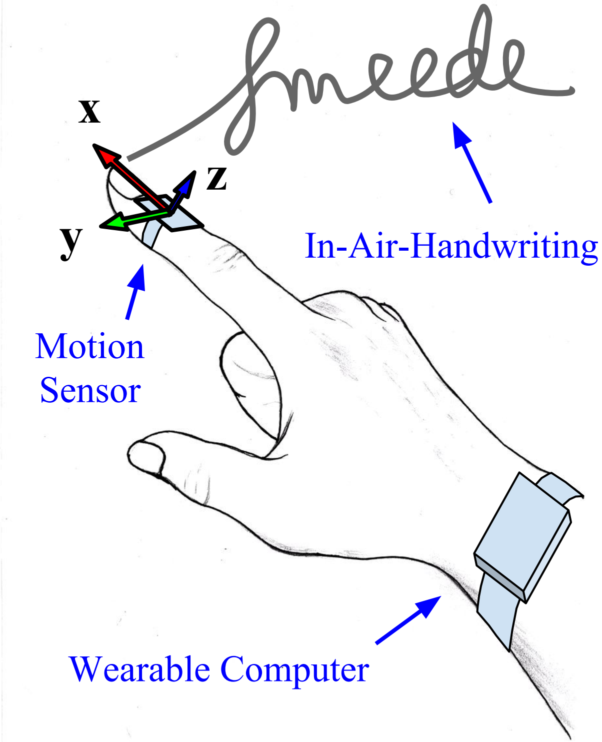
ΔL: **length difference**

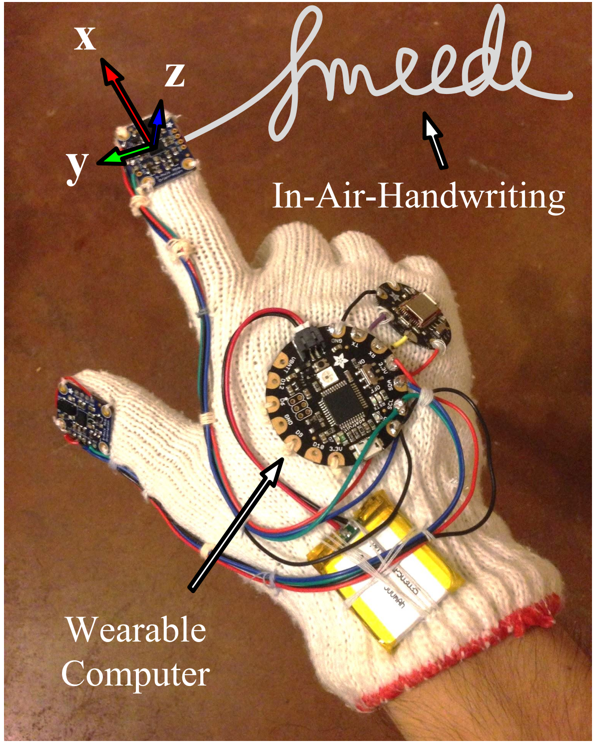


"accept" or "reject"

SVM

Device Prototype - data glove





engineering.asu.edu

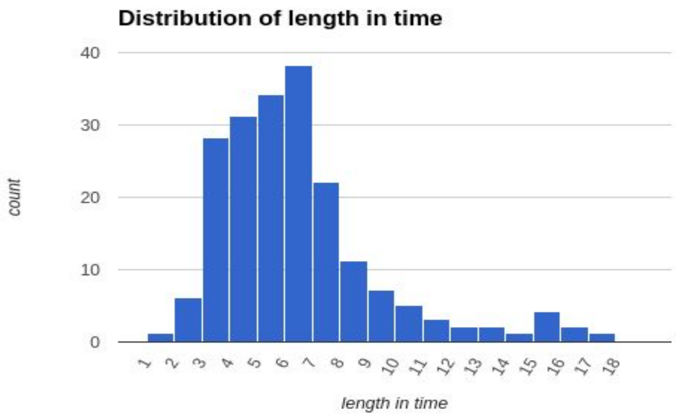
Datasets

200 passcodes created and written by 116 users, 5 + 5 repetitions.
7 impostors to mimic the writing of all 200 passcodes, 5 repetitions each.
21 passcodes by 7 users are tracked for 4 weeks, on average twice a week, 5 repetitions each time.

three classes:

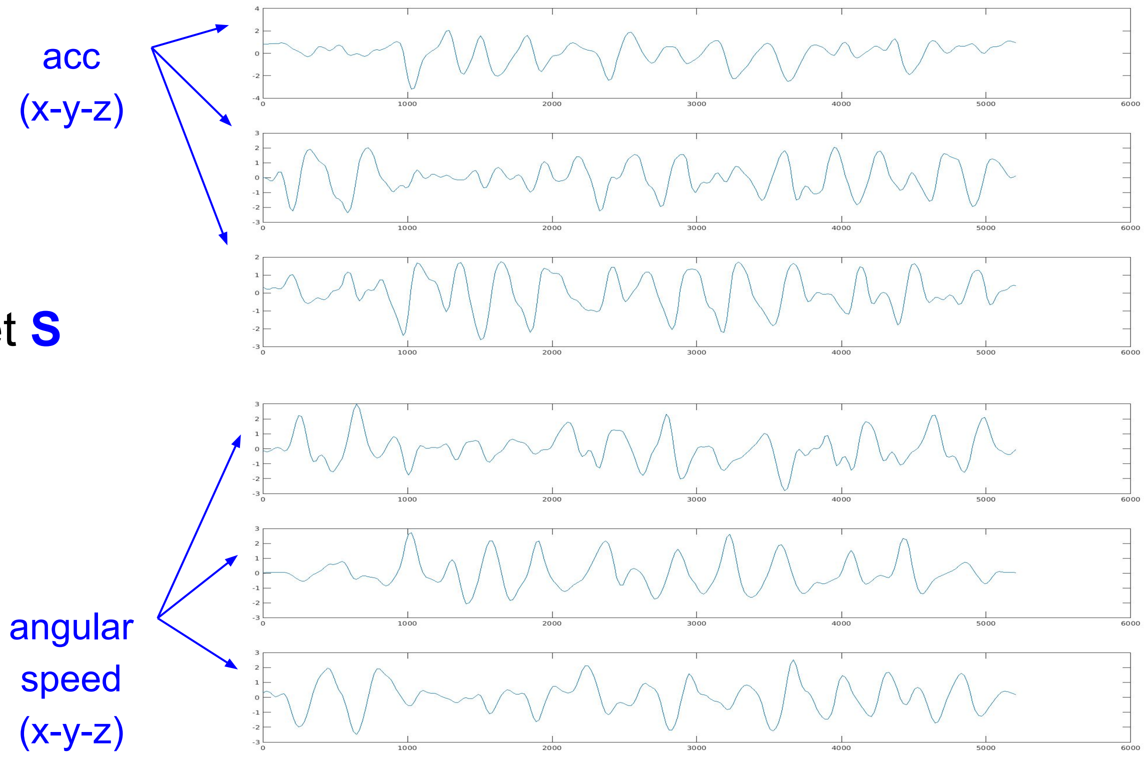
- true-user: S and T are from the same account
- false-user: S and T are from different accounts
- spoof: S is from the impostors

S is the signal in the request, T is the template



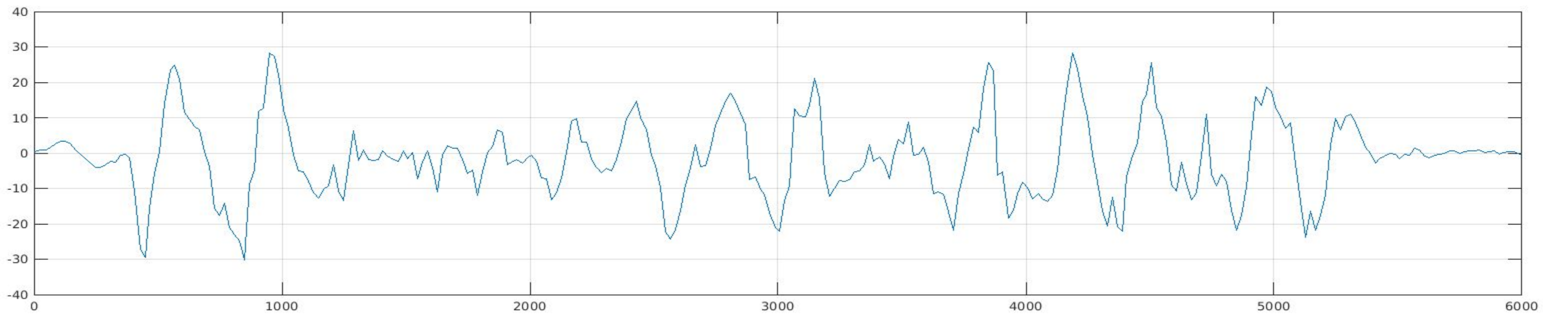
Signal Model

- **R** is d × l matrix
  - d is sensor dimension
  - l is signal length
- **R** is preprocessed to get **S**
  - Trim
  - Low-Pass Filter
  - Normalize
  - Alignment

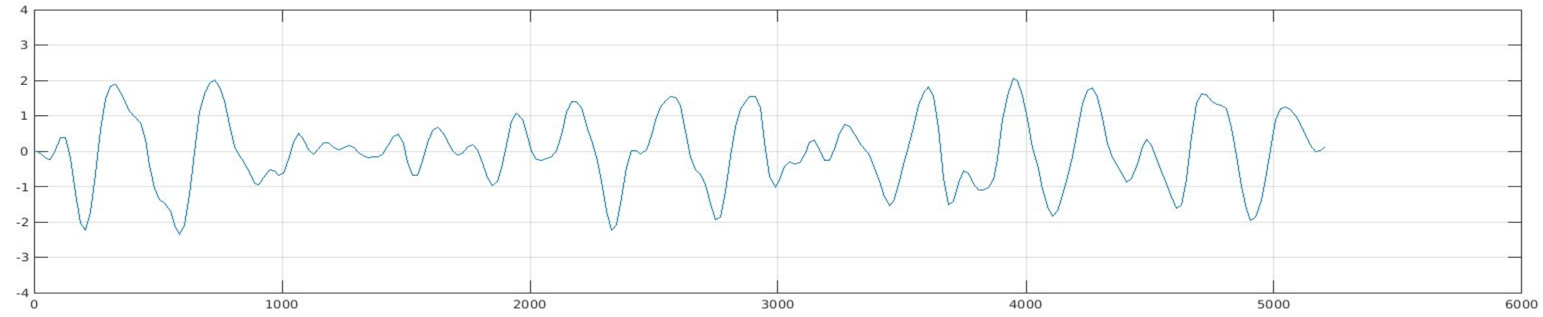


Preprocessing Example

Before preprocessing

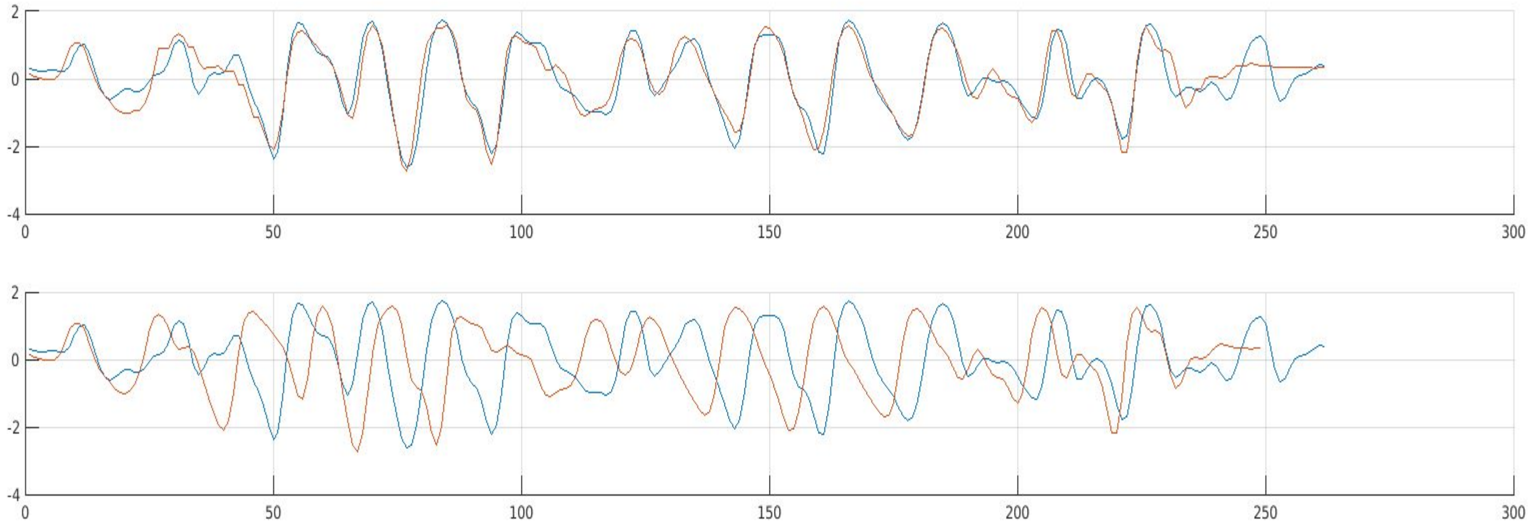


After preprocessing



Alignment Example

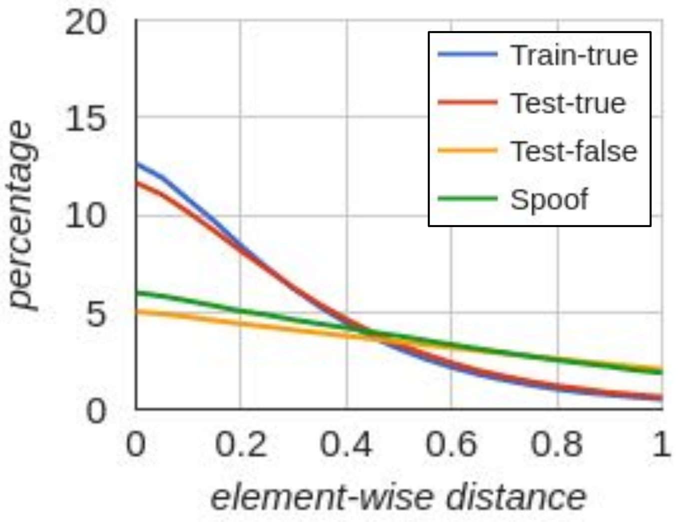
After alignment



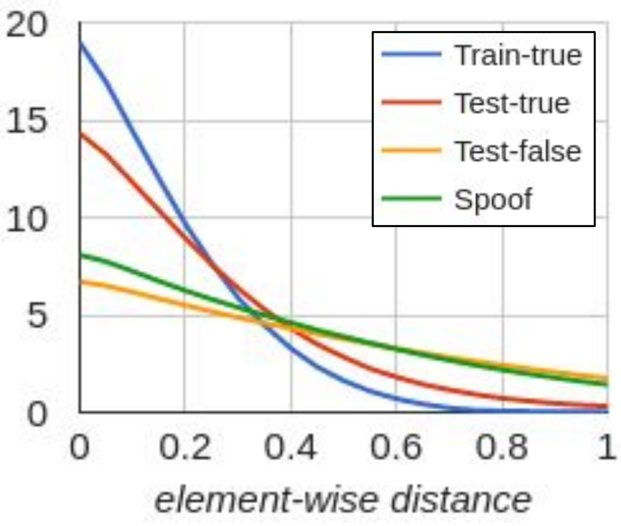
Before alignment

Temporal Distance

- $D_{ij} = | S_{ij} - T_{ij} |$
- **TD** = histogram($D_{ij} * k_1 * k_2$)



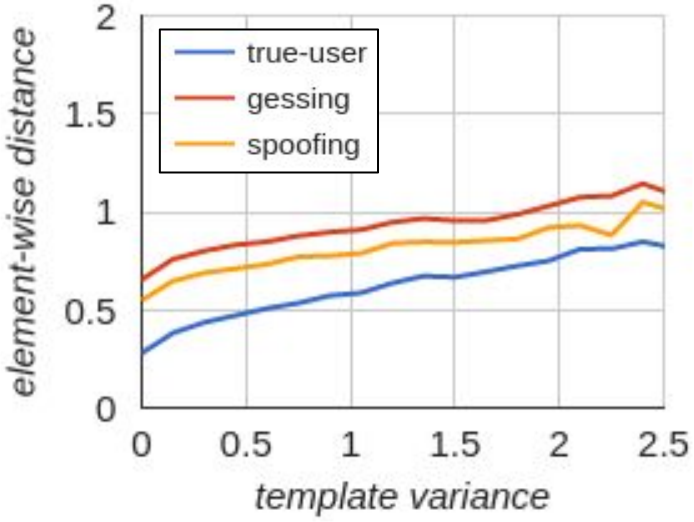
TD before scaling



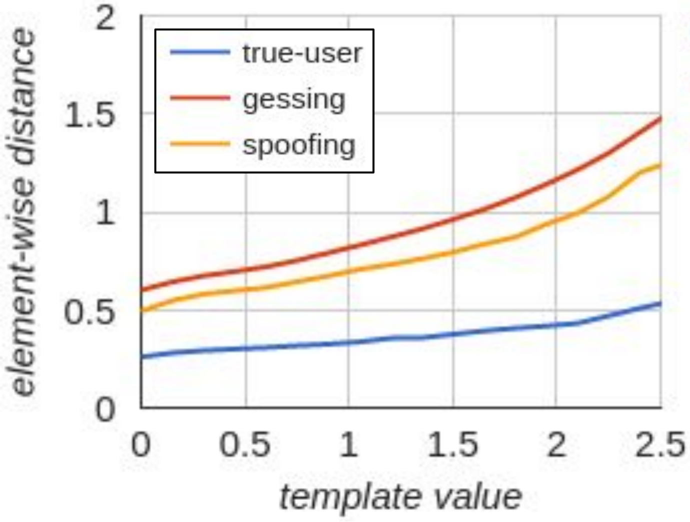
TD after scaling

Distance Scaling

- $k_1 = 1 / (1 + w_1 * C_{ij})$



- $k_2 = 1 / (1 + w_1 * T_{ij})$

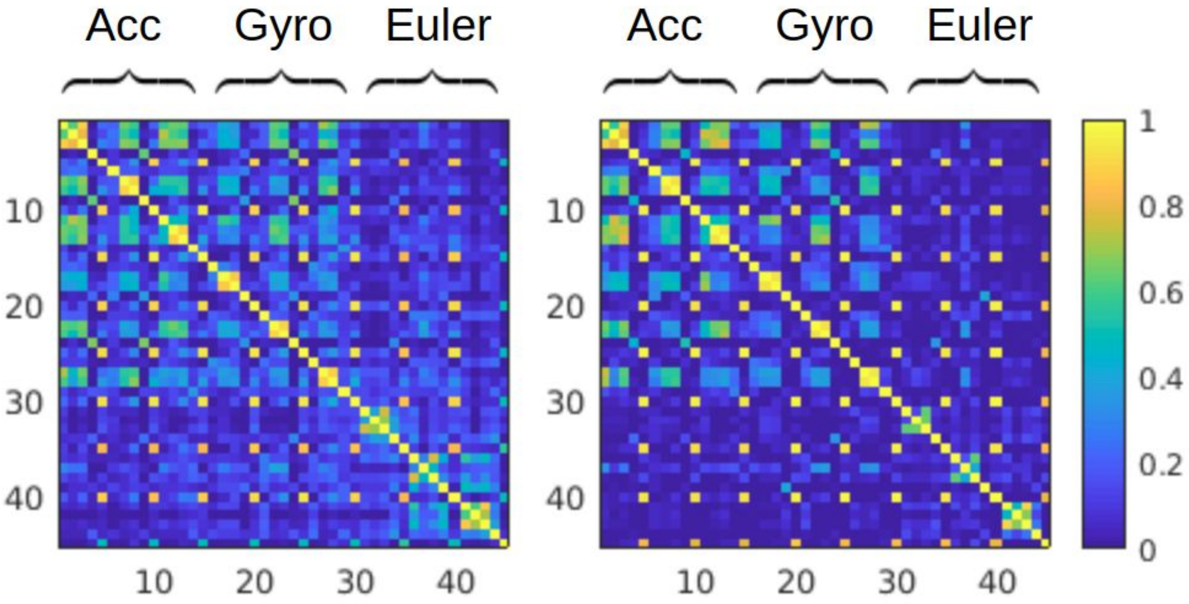


Statistical Similarity

$\mathbf{SS} = (\Delta\mathbf{M}, \Delta\mathbf{\Sigma}, \Delta\mathbf{P}, \Delta\mathbf{\Lambda}, \Delta\mathbf{H})$

- **Mean:** Mean of each sensor axis, $\mathbf{M} = (\mu_1, ..., \mu_d)$, where $\mu_j = \text{mean}(S_j)$.
- **Variance:** Variance of each sensor axis, $\mathbf{\Sigma} = (\sigma_1, ..., \sigma_d)$, where $\sigma_j = \text{var}(S_j)$.
- **Correlation:** Correlation among sensor axes, $\mathbf{P} = (\alpha_{xy}, \alpha_{yz}, \alpha_{xz}, \beta_{xy}, \beta_{yz}, \beta_{xz}, \gamma_{xy}, \gamma_{yz}, \gamma_{xz})$, where α_{xy} , β_{xy} , γ_{xy} is the correlation of acc, gyro, Euler axis x and y
- **Amplitude:** Sum of amplitude of each axis, $\mathbf{\Lambda} = (\lambda_1, ..., \lambda_d)$, where $\lambda_j = \Sigma|S_{ij}|$.
- **Entropy:** Entropy of each axis (treat S_{ij} as random variable), $\mathbf{H} = (\eta_1, ..., \eta_d)$, where $\eta_j = - \Sigma_i\, p(S_{ij}) \log_2 p(S_{ij})$

Statistical Features Correlation

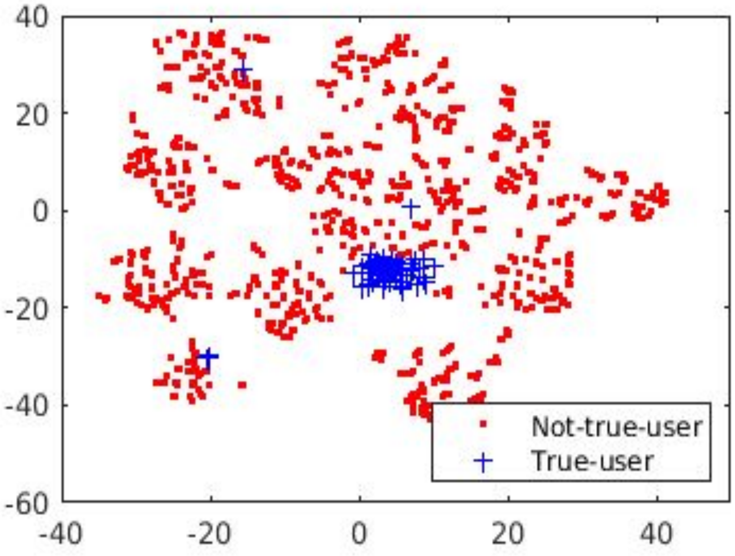


true-user class

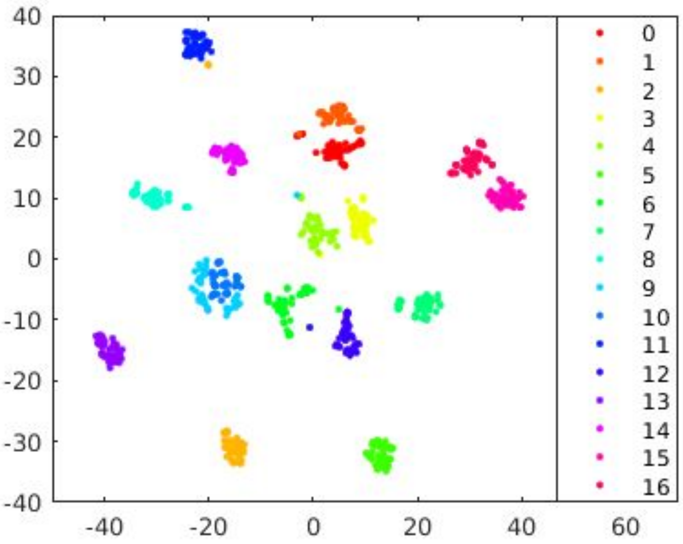
false-user class

Visualization (t-SNE)

The signals from the same accounts clustered in the statistical feature space.



Statistical Similarity



Statistical Features of Signals from 17 Accounts

Features and Classification

- Temporal Distance

  $\mathbf{TD} = \text{histogram}(D_{ij} * k_1 * k_2)$

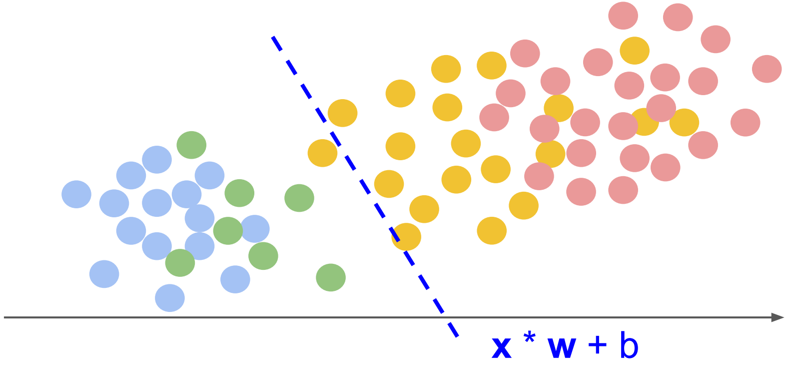
- Statistical Similarity

  $\mathbf{SS} = (\Delta\mathbf{M}, \Delta\mathbf{\Sigma}, \Delta\mathbf{P}, \Delta\mathbf{\Lambda}, \Delta\mathbf{H})$

- Length Difference

  $\Delta L = |\, \text{len}(\mathbf{S}) - \text{len}(\mathbf{T}) \,| \,/\, \text{len}(\mathbf{T})$

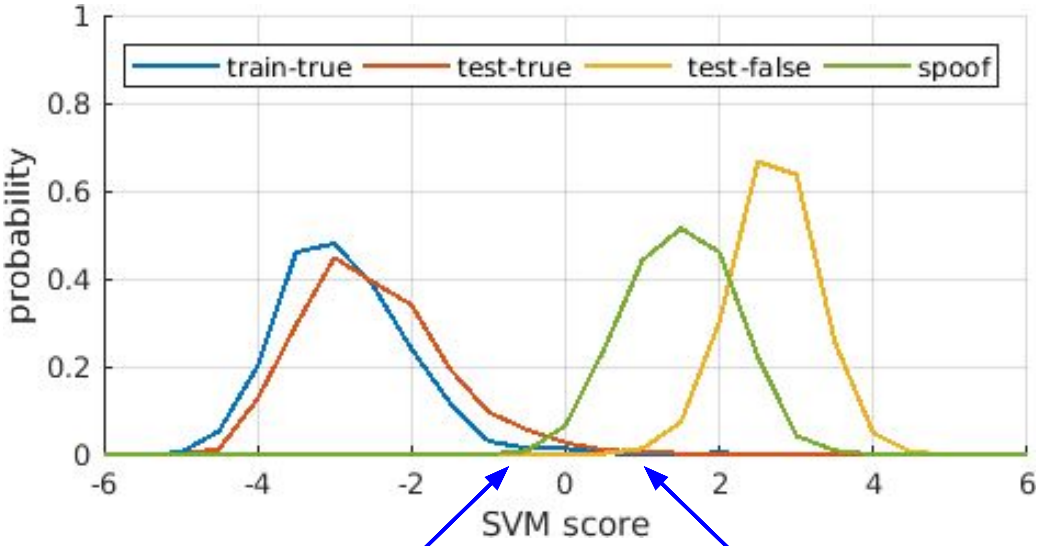
Final feature vector $\mathbf{x} = (\mathbf{TD}, \mathbf{SS}, \Delta\mathbf{L})$



Using binary soft margin SVM classifier

if **x** * **w** + b < decision_threshold
    accept.
else
    reject.

Score distribution with temporal distance



0.42% overlap between true-user and false-user

3.1% overlap between true-user and spoof

Classification Results

one SVM model for all accounts

per account SVM model

Classifier	EER	EER (spoof)	FMR 10K	FMR 100K	Zero -FMR
SVM(TD)	0.2%	1.4%	1.8%	3.6%	5.1%
SVM(TD, SS)	0.2%	1.4%	1.5%	2.8%	3.9%
SVM*(TD, SS)	**0.1%**	**1.4%**	**0.5%**	**0.7%**	**1.5%**
DTW(baseline)	0.4%	4.2%	4.4%	8.4%	16.4%

Reasons for performance improvement over DTW:

- Our method exploits the large passcode capacity and rich information in the in-air-handwriting.
- Consistency in hand movement by eliminating constraints helps performance.
- Higher quality of motion signal, better preprocessing technique help performance further.
- Good features, efficient classifier.

Conclusions

- In-Air-Handwriting based authentication has good potentials.

Limitations

- Behavior change in the long term
- Template protection and template update

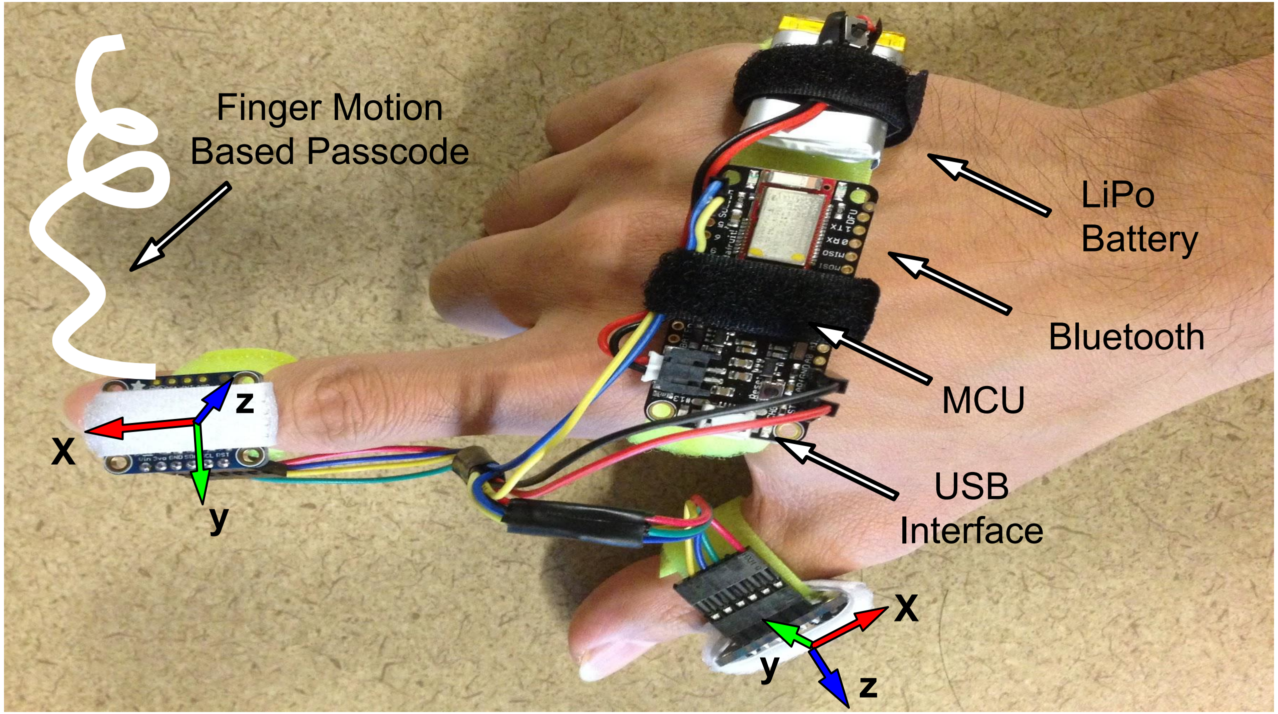
Future Work

- More data with longer time span to study the behavior persistence.
- Using a different type of sensor, e.g., a depth camera.
- Template encryption by a key directly generated from the in-air-writing signal

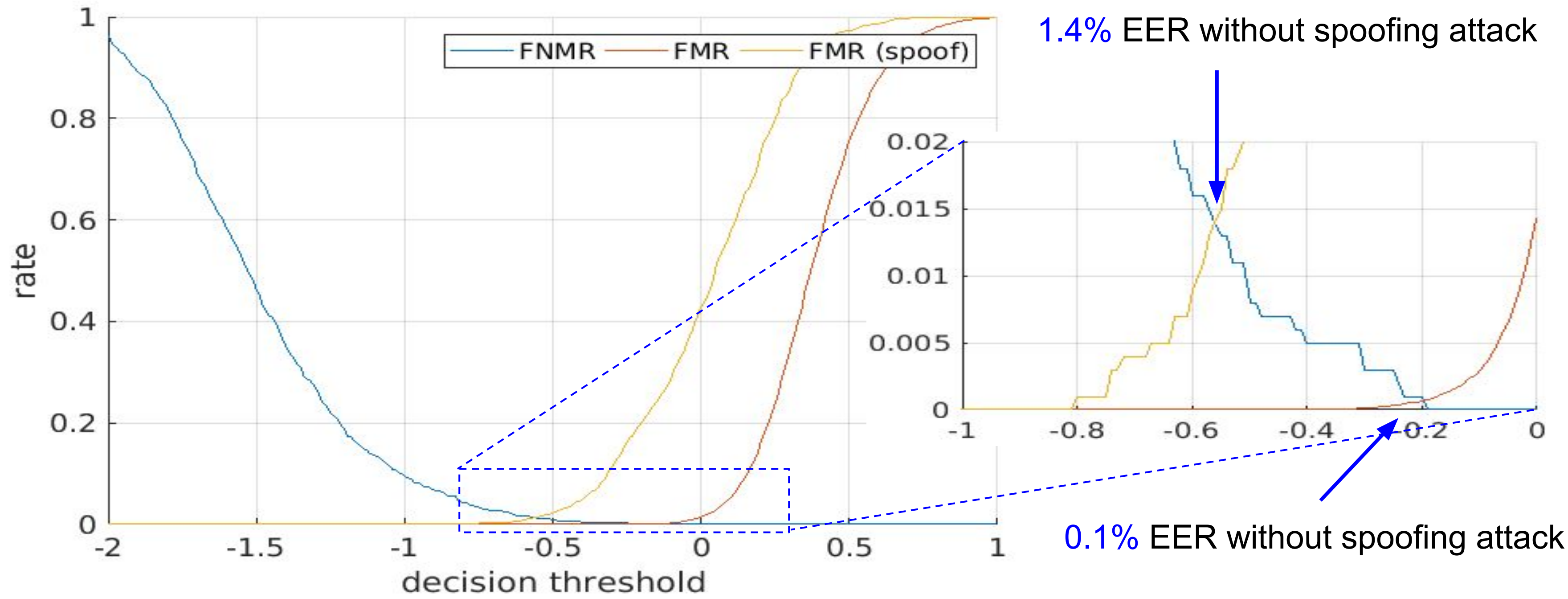
Thank you!

Q & A

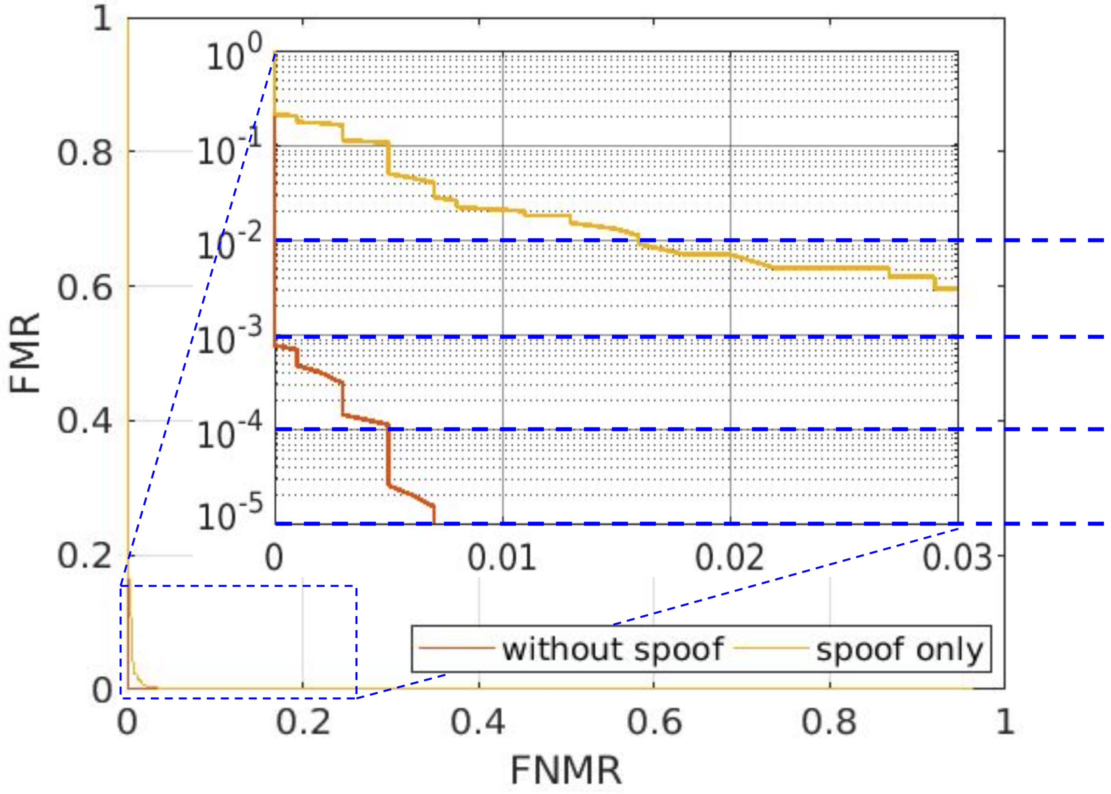
Device Prototype - ver. 2 - hand band



False Non-Match Rate (FNMR) and False Match Rate (FMR)

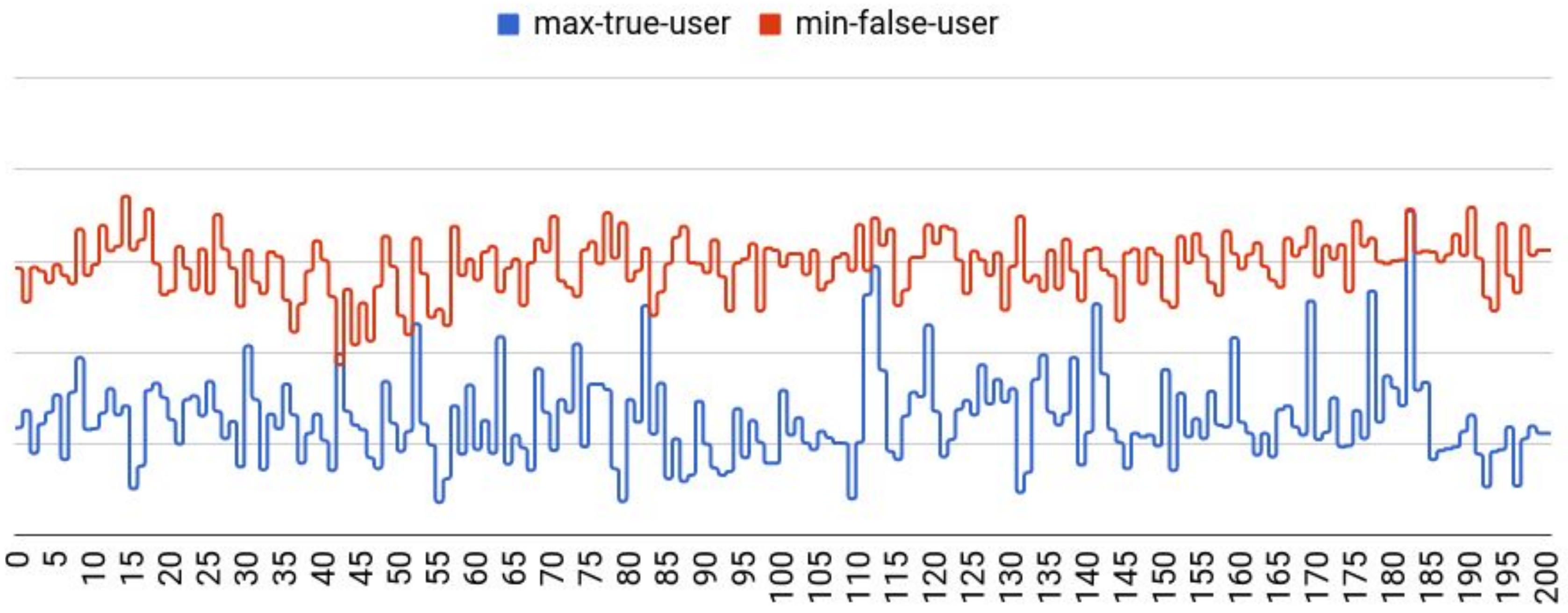


Receiver Operating Characteristic (ROC)



	without spoof	spoof only
FMR 100	< 0.01%	(1.6%)
FMR 1000	= 0.1%	(9.4%)
FMR 10K	= 0.5%	
FMR 100K	= 0.7%	
Zero FMR	= 1.5%	

Classification results of each account (one model)



Classification results of each account (one model)