KinWrite: Handwriting-based Authentication Using Kinect

Jing Tian*, Chengzhang Qu **, Wenyuan Xu* and Song Wang*

*Dept. of Computer Science and Engineering, University of South Carolina

**School of Computer Science, Wuhan University

Roadmap

- Authentication Background
- KinWrite Framework
  - Data processing
  - Enrollment & Verification
- Experiments
  - Legitimate users
  - Attackers
- Conclusions & On-going work

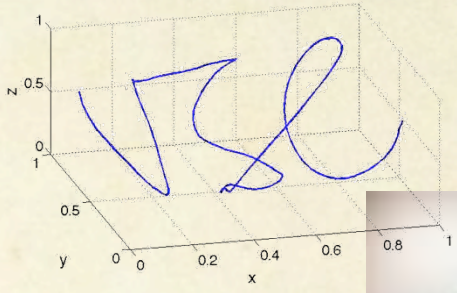
Authentication Background

- What you know – text passwords
  - What is secure is hard to remember
- What you own – token
  - Lost or stolen token
- Who you are – Physical biometrics
  - Limited number

Goal: address all the limitation.

Our Solution: *3D-Signature*

- **3D signature**: *handwriting in 3D space*
  - Write **short**, **easy to remember** passwords in the space,
    - 2 or 3 characters
  - Behavioral biometrics:
    - Can be updated
    - Difficult to duplicate
    - A weak typed password can still be strong if it is written in 3D space

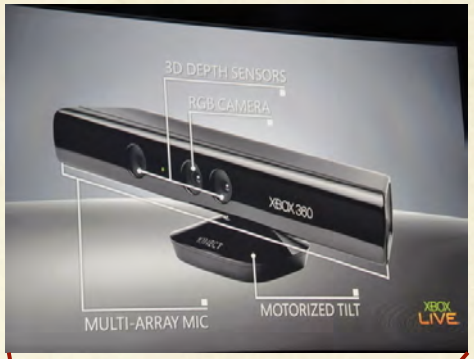


- Challenges:
  - Change over time?
  - Reject malicious users?
  - Accept genuine users?

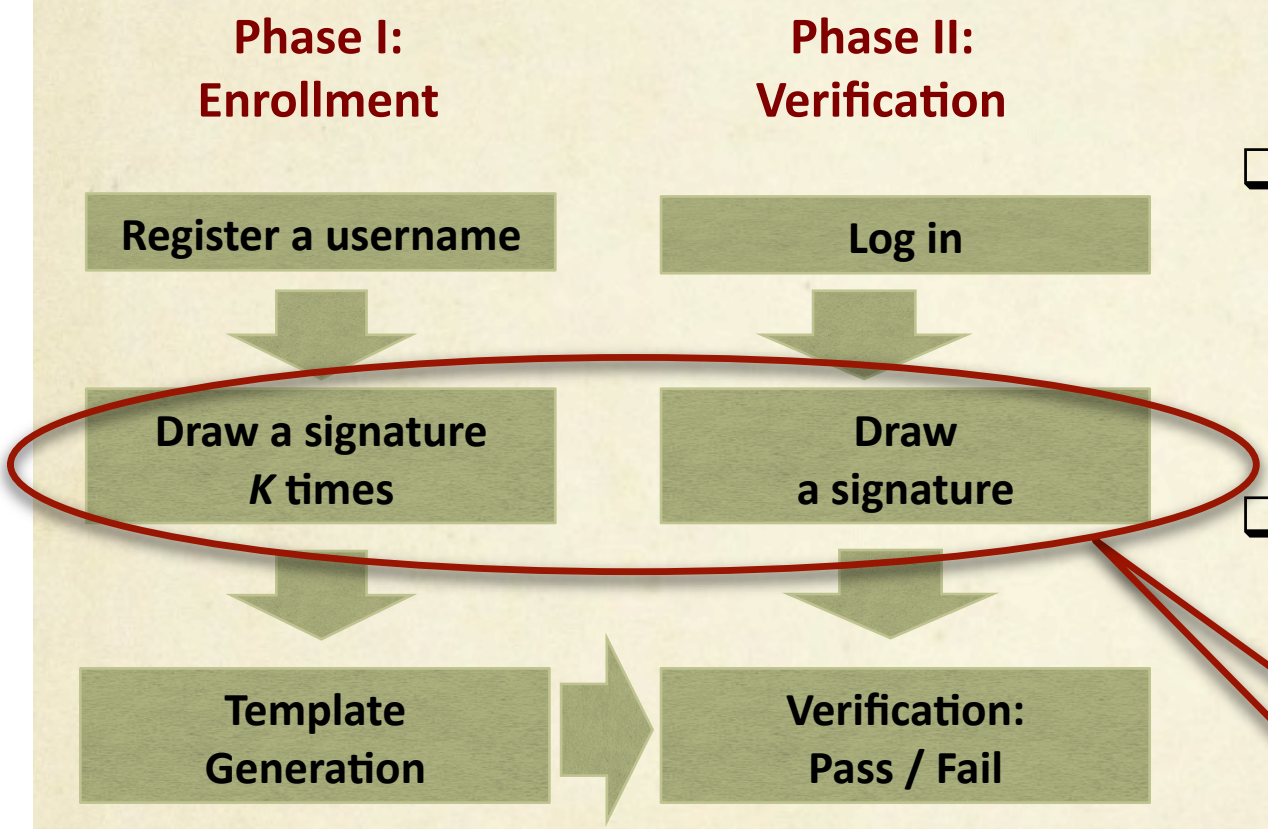
Our Solution: KinWrite

-- *Kinect + 3D-Signature*

- Microsoft Kinect
  - A motion input RGB-D sensor
  - Launched by Microsoft for Xbox 360 and Windows PCs
  - Advantages
    - Low cost
    - Captures 3D information
      - Depth sensor
    - Works in the dark
  - Disadvantages
    - Low resolution
    - Measurement errors



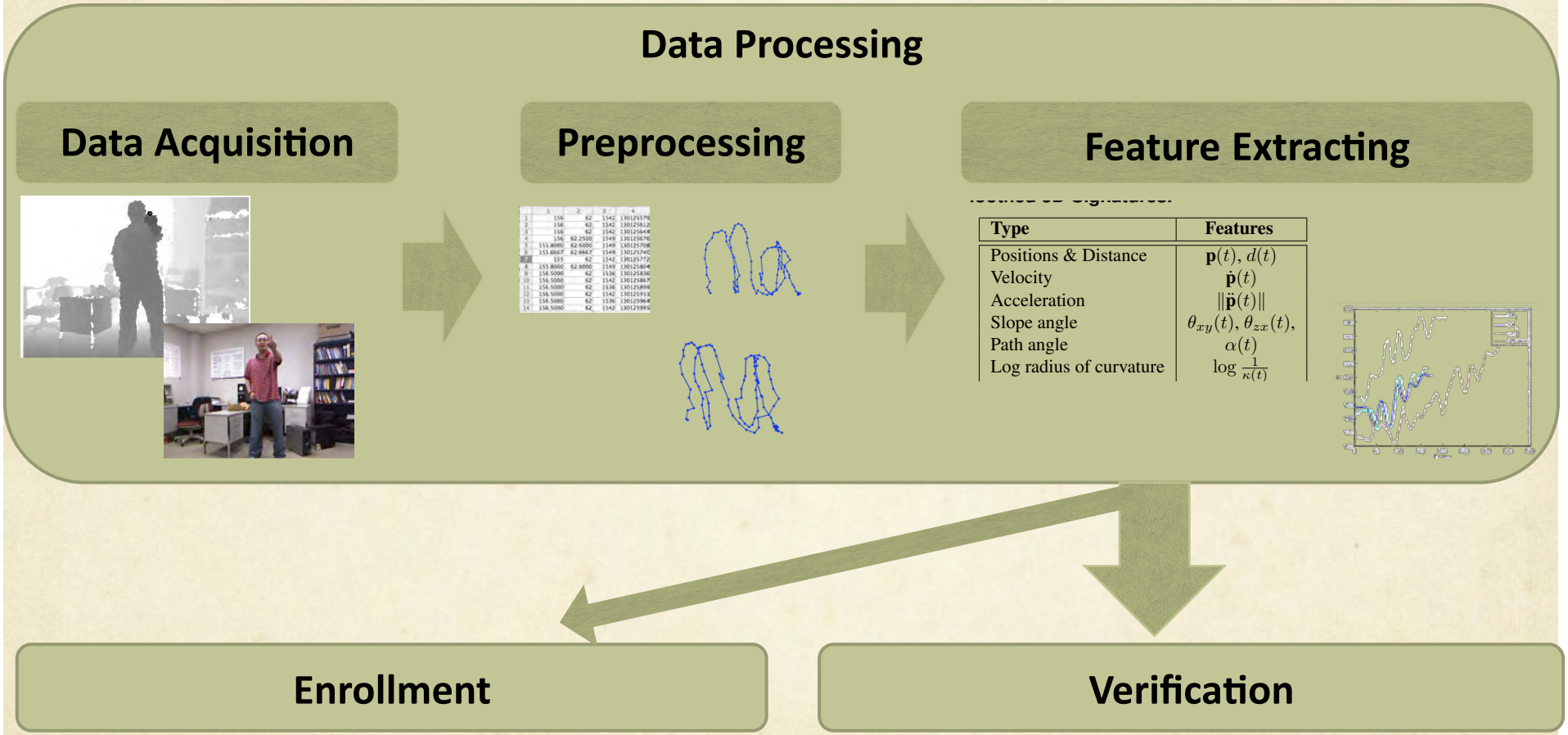
KinWrite: Overview



- Usability requirements
  - Rapid enrollment
  - Rapid verification
- Security requirement
  - Unforgeability

3D Signatures should be processed

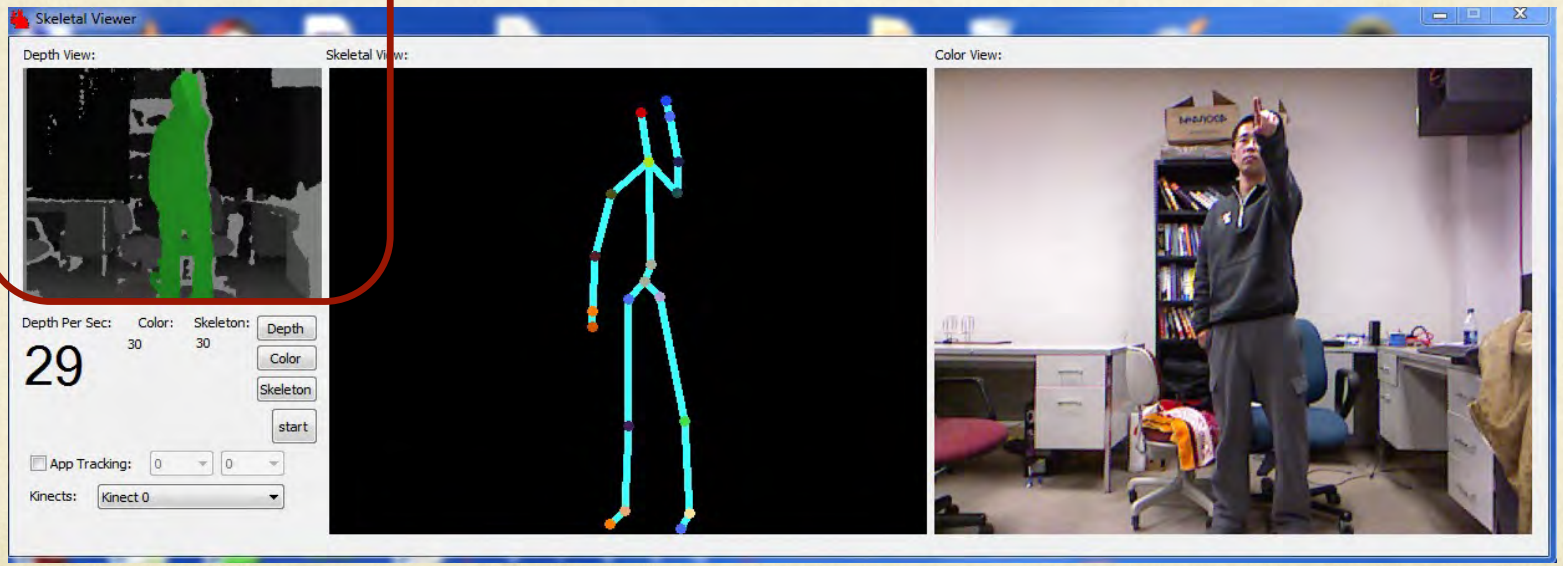
KinWrite: Data Processing



Data Processing: Acquisition

- Subject: raise a hand and use a fingertip
- Kinect: record the writing motion in the space

Depth frames **Skeleton points** **RGB images**

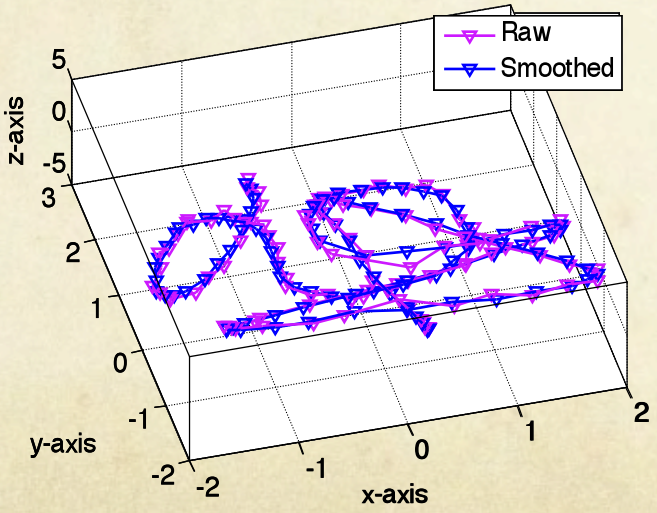


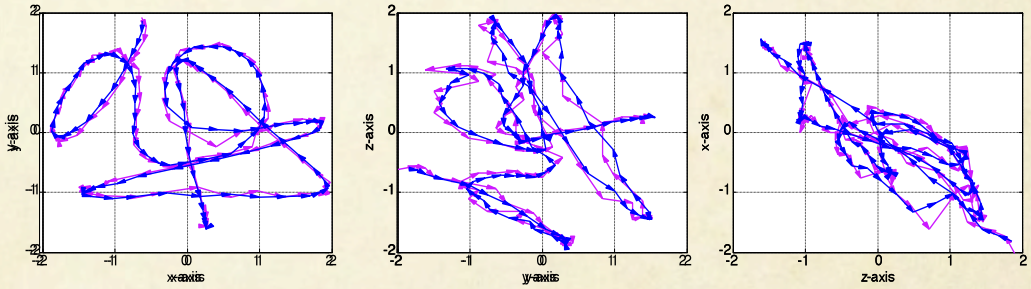
Data Acquisition → Data Preprocessing → Feature Extracting

Data Processing: Preprocessing

Fingertip position 1
Fingertip position 2
...
Fingertip position n

- Raw signatures
  - Noisy
- Smooth
  - Kalman filter



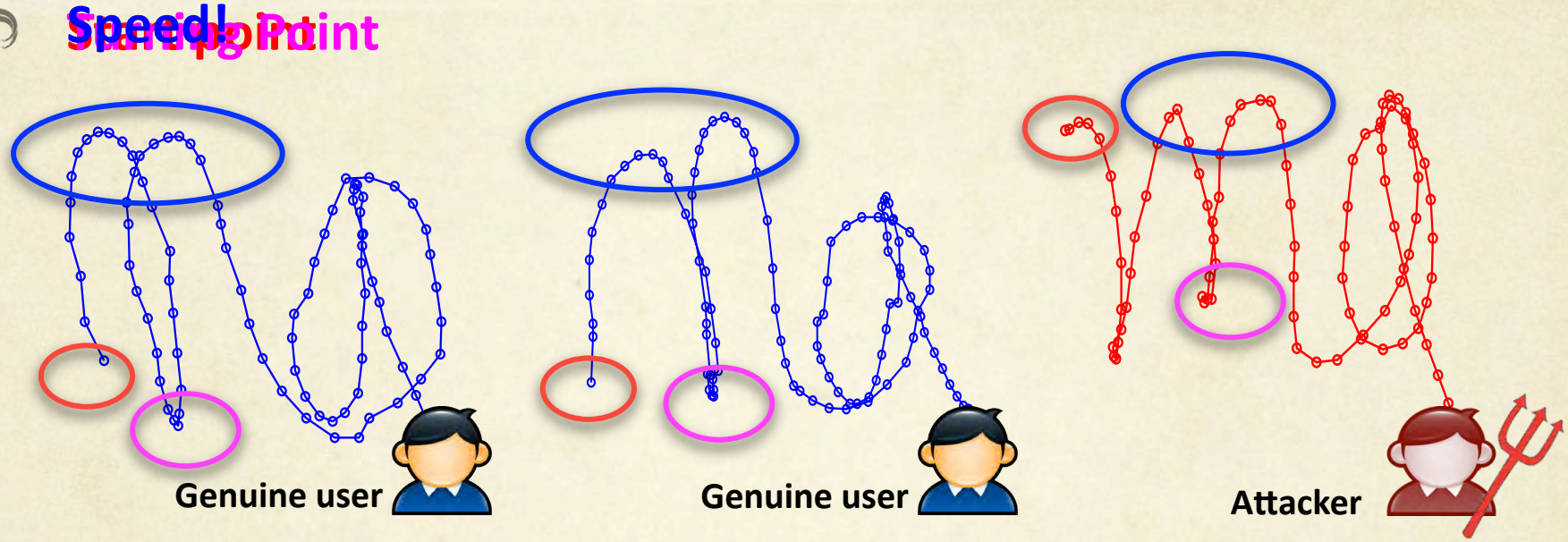


x-y plane y-z plane z-x plane

Data Acquisition → **Data Preprocessing** → **Feature Extracting**

Data Processing: Feature Extracting

- Speed!



Type	Features
Positions & Distance	$\mathbf{p}(t), d(t)$
Velocity	$\dot{\mathbf{p}}(t)$
Acceleration	$\|\ddot{\mathbf{p}}(t)\|$
Slope angle	$\theta_{xy}(t), \theta_{zx}(t),$
Path angle	$\alpha(t)$
Log radius of curvature	$\log \frac{1}{\kappa(t)}$

← ***Six types 3D features***

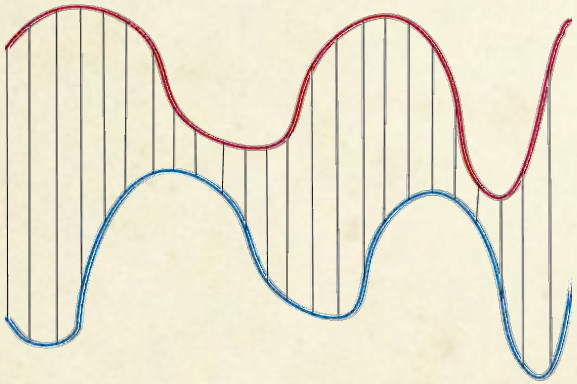
- *Movement*
- *Geometry*

Data Acquisition → Data Preprocessing → Feature Extracting

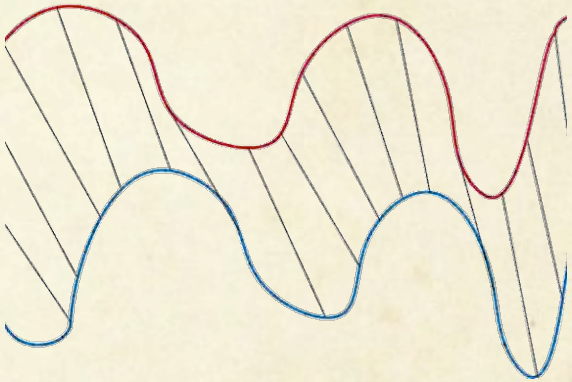
Quantify the similarity of 3D-signatures

Approach--Dynamic Time Warping (DTW)

- DTW distance represents the similarities between two 3D-signature samples --Warping along the temporal axis



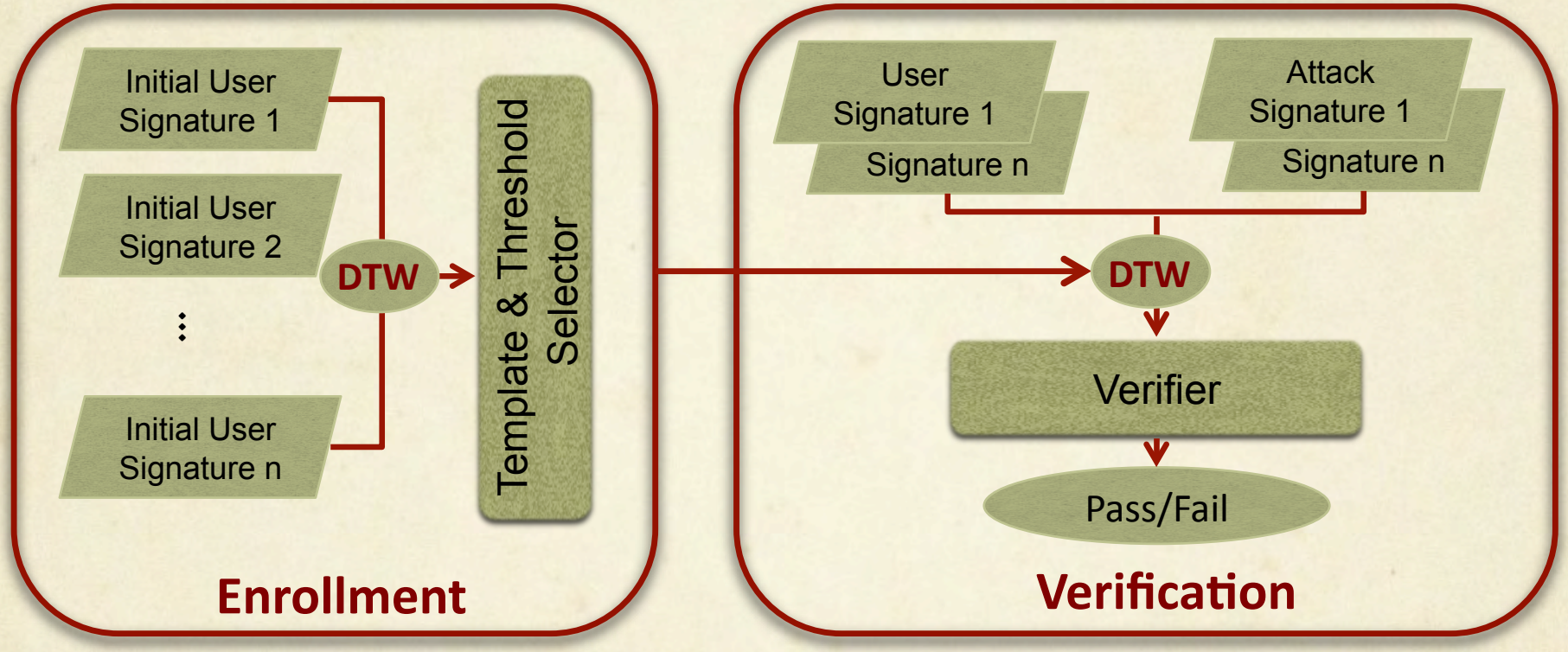
Euclidean Distance



Dynamic Time Warping

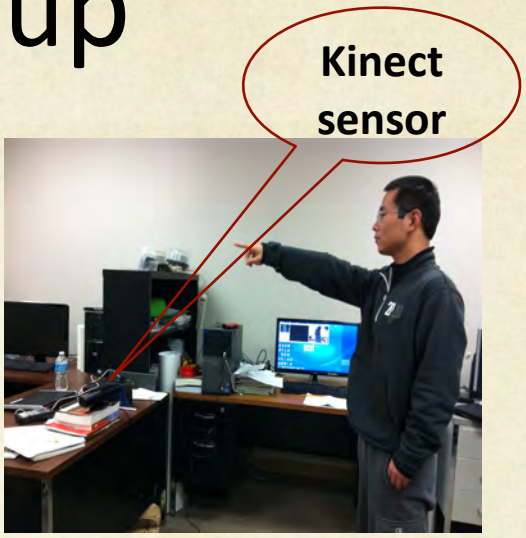
- Requires a small number of training samples

KinWrite: Enrollment & Verification



- **Template:** best represent the signature
- **Threshold:** determine whether two signatures are from the same user
  - DTW distance **<** threshold → pass
  - DTW distance **>** threshold → fail to pass

Experiments: Setup



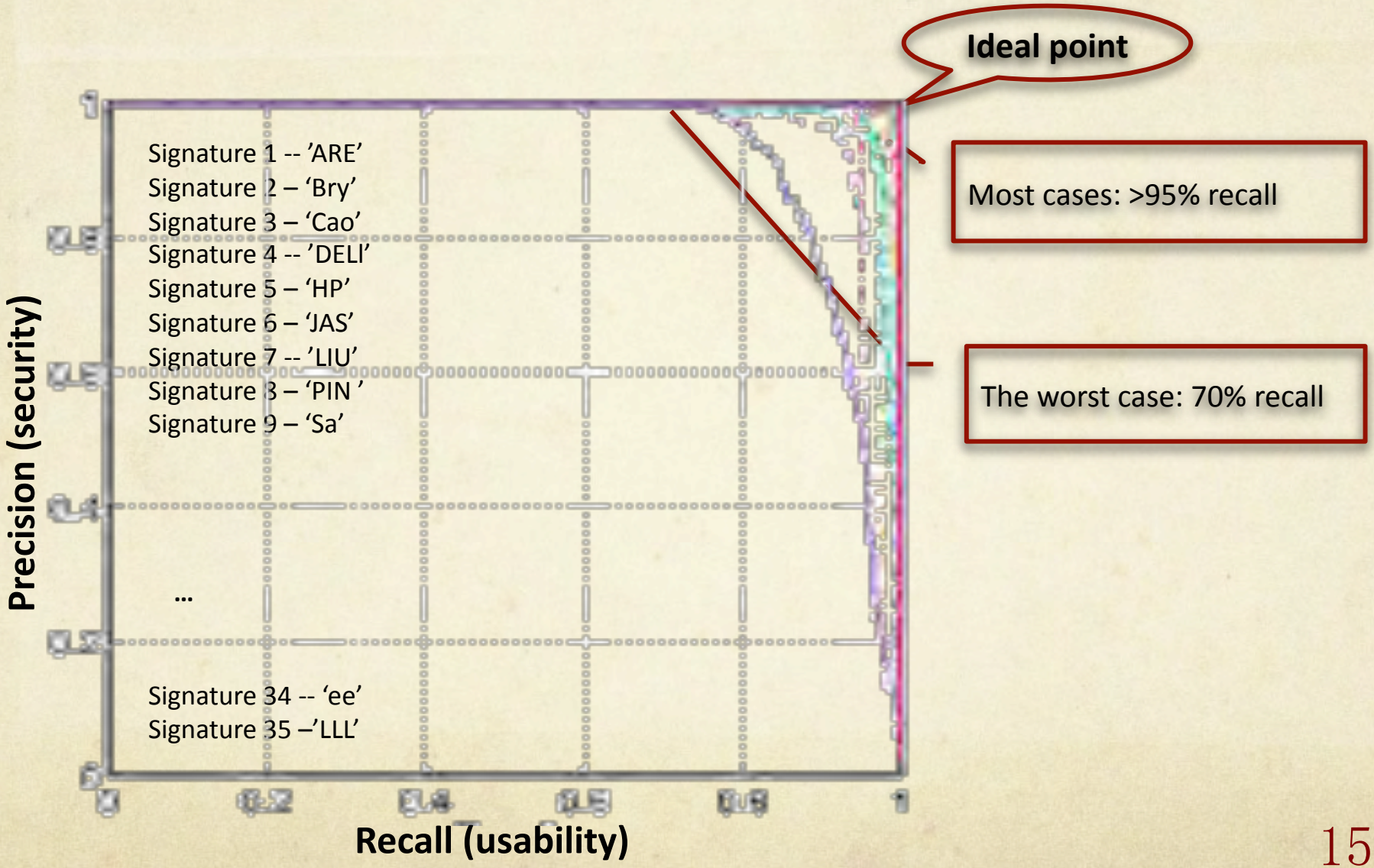
- Experiment setup
  - 3 Kinect sensors
  - Distance → 1.5 - 2.5 meters
  - A sample → a video clip (2-12s),
    ~30 frames/second, depth frames
- Evaluation metrics:
  - *Precision* = verified genuine users **/** all verified users
    - Security
  - *Recall* = verified genuine users **/** all genuine users
    - *Usability*
    - *Average attempts = 1 / Recall*

Experiments: Scenarios

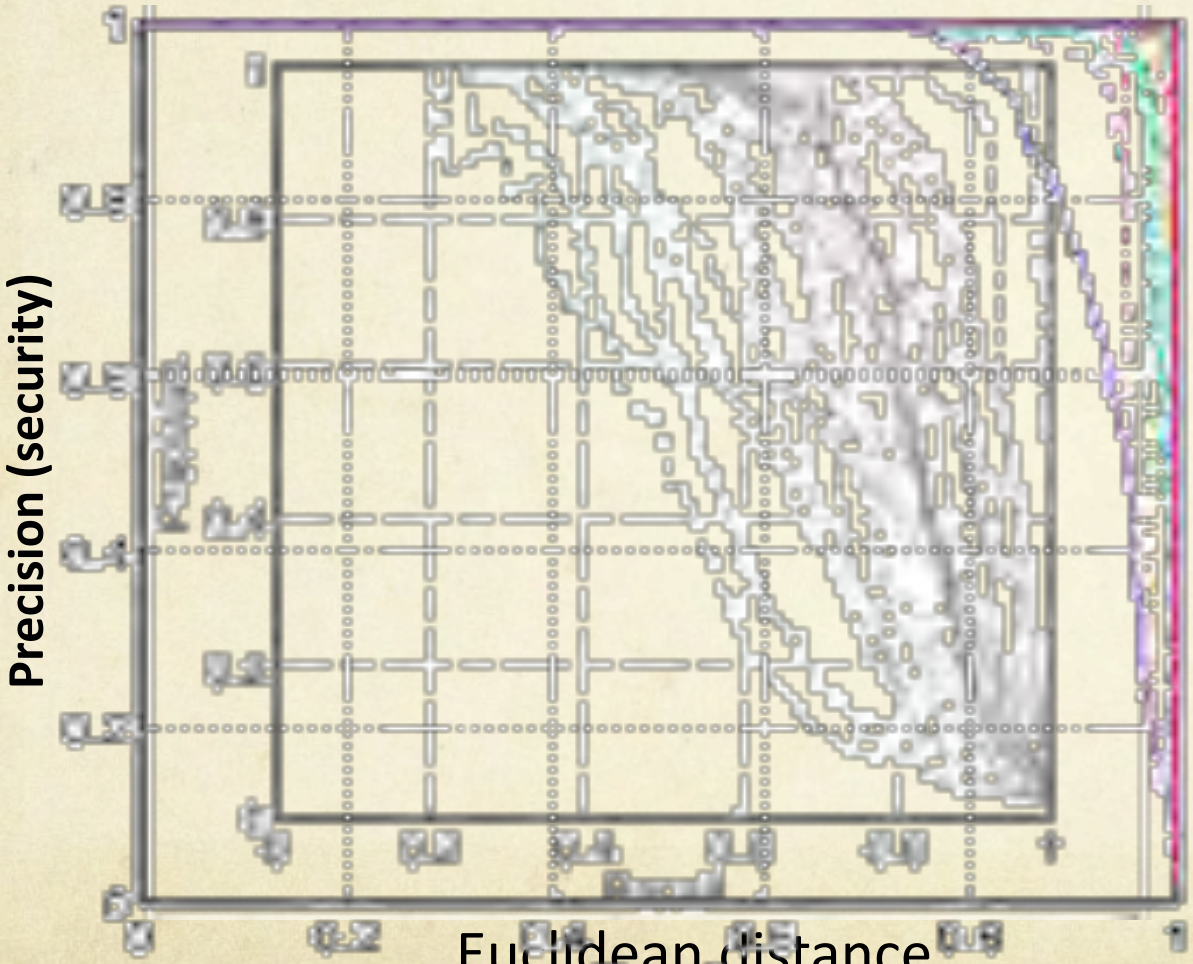
- Scenario 1 – Legitimate users

  - Let the subjects write their genuine signatures:
    - **18** users, **35** signatures
    - **18 - 47** 3D-signature *samples* for each signature over a period of **5** months
    - **1180** samples in total

Results: Legitimate Users



Results: Legitimate Users

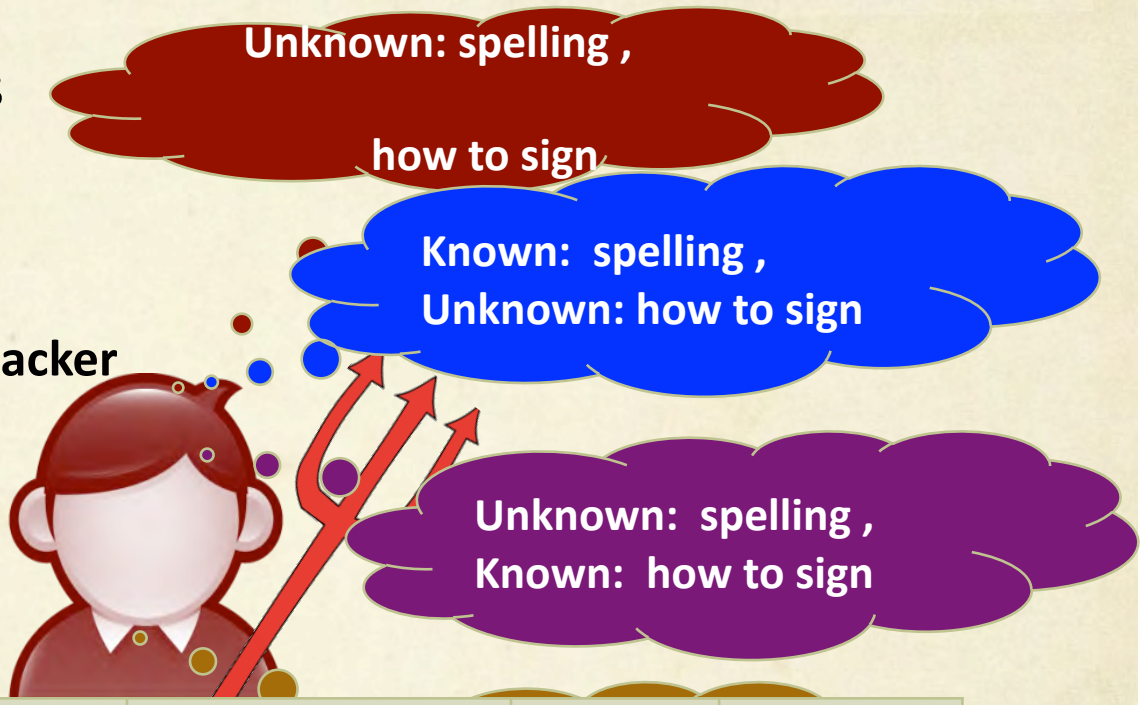


Euclidean distance

DTW

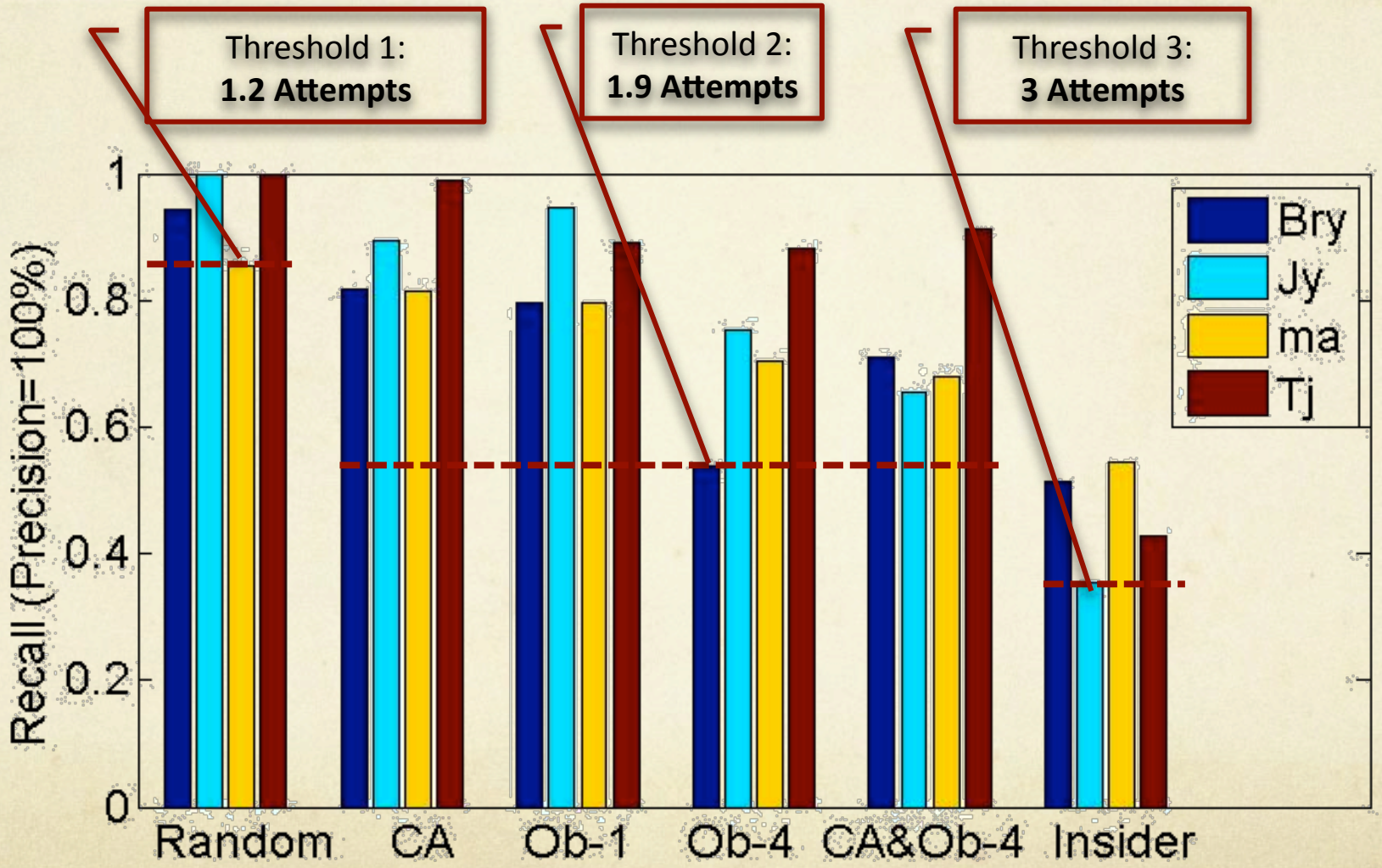
Experiments: Scenarios

- Scenario 2 – Attackers
  - Attack model
    - **Random attacker**
    - **Content-aware attacker**
    - **Observer attacker**
    - **Educated attacker**
    - **Insider attacker**



Attack Type	# 'attacker'	# samples from each	# 'victim'	# samples
Random Attack	34	14~42	4	1040
Content-Aware Attack	6	10	4	240
1-Observer Attack	12	5	4	240
4-Observer Attack	12	5	4	240
Educated Attack	12	5	4	240
Insider Attack	12	5	4	240

Results: Attack Scenarios



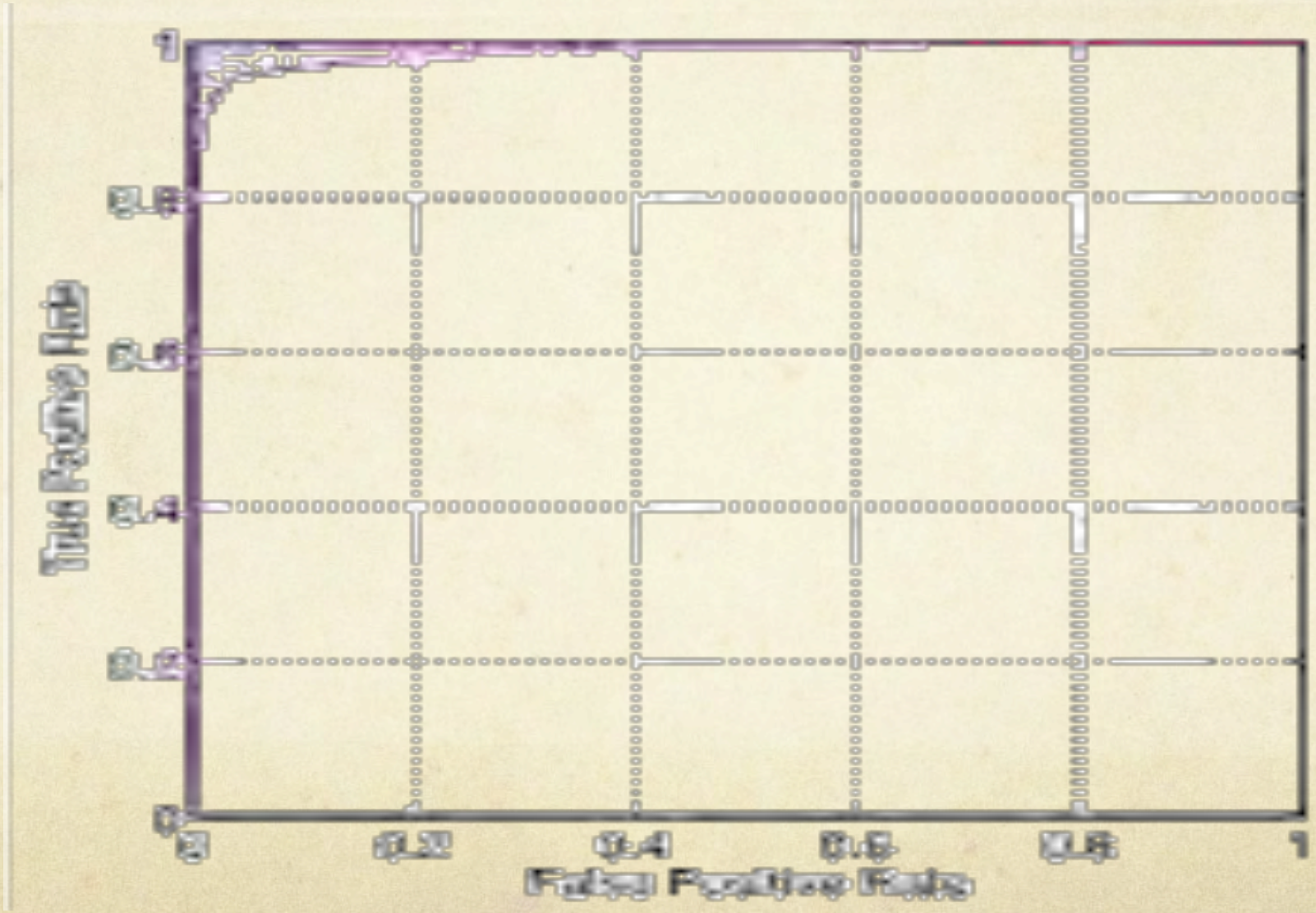
Conclusions and On-going Work

- Conclusions
  - Designed a behavior-based authentication system (KinWrite)
  - Our experiment results based on over 2000 samples showed that 3D-signatures can be used to verify users
- On-going Work
  - Compare usability among 3D signatures and existing authentication methods
  - Study other types of 3D signatures

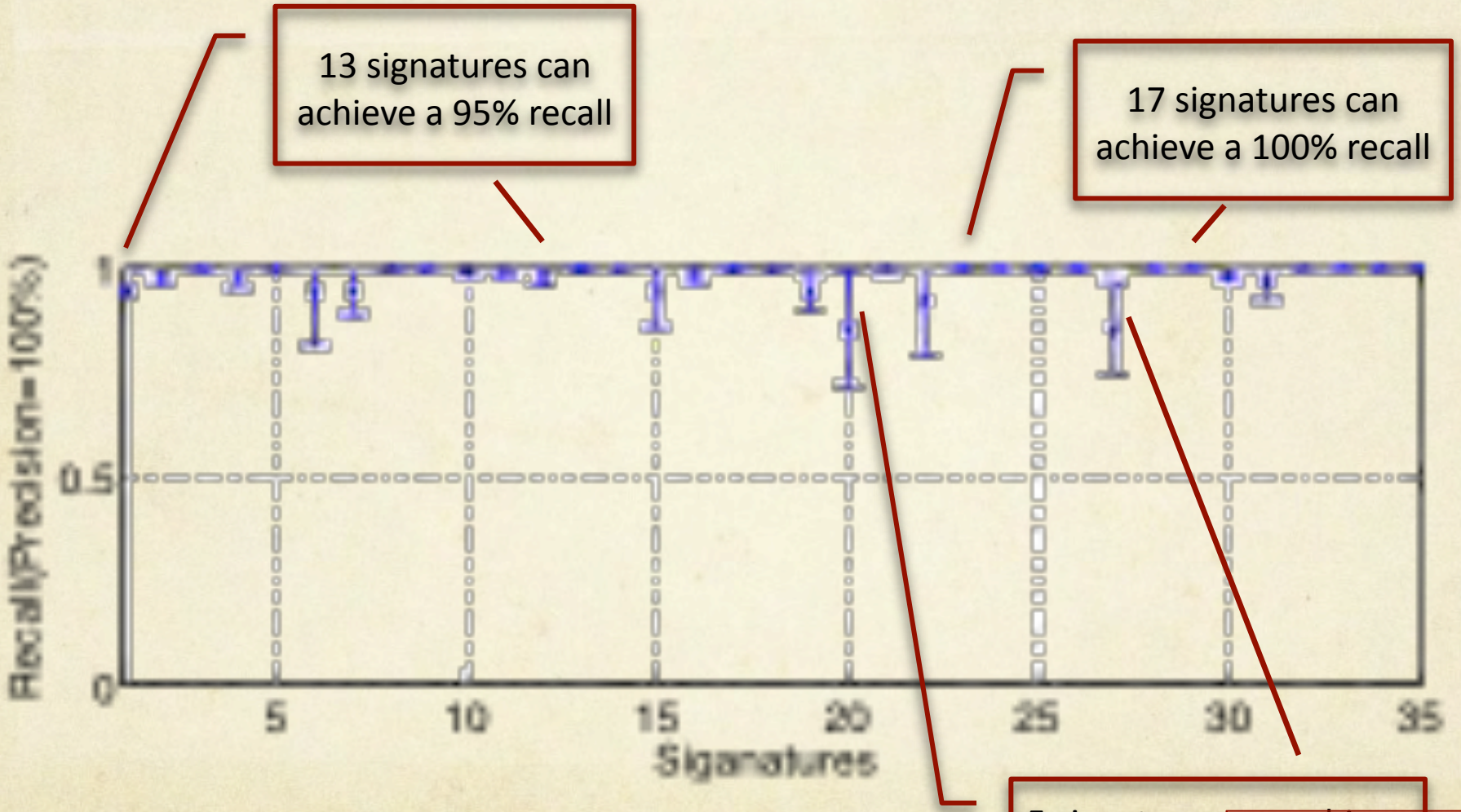
Thank you!

Questions?

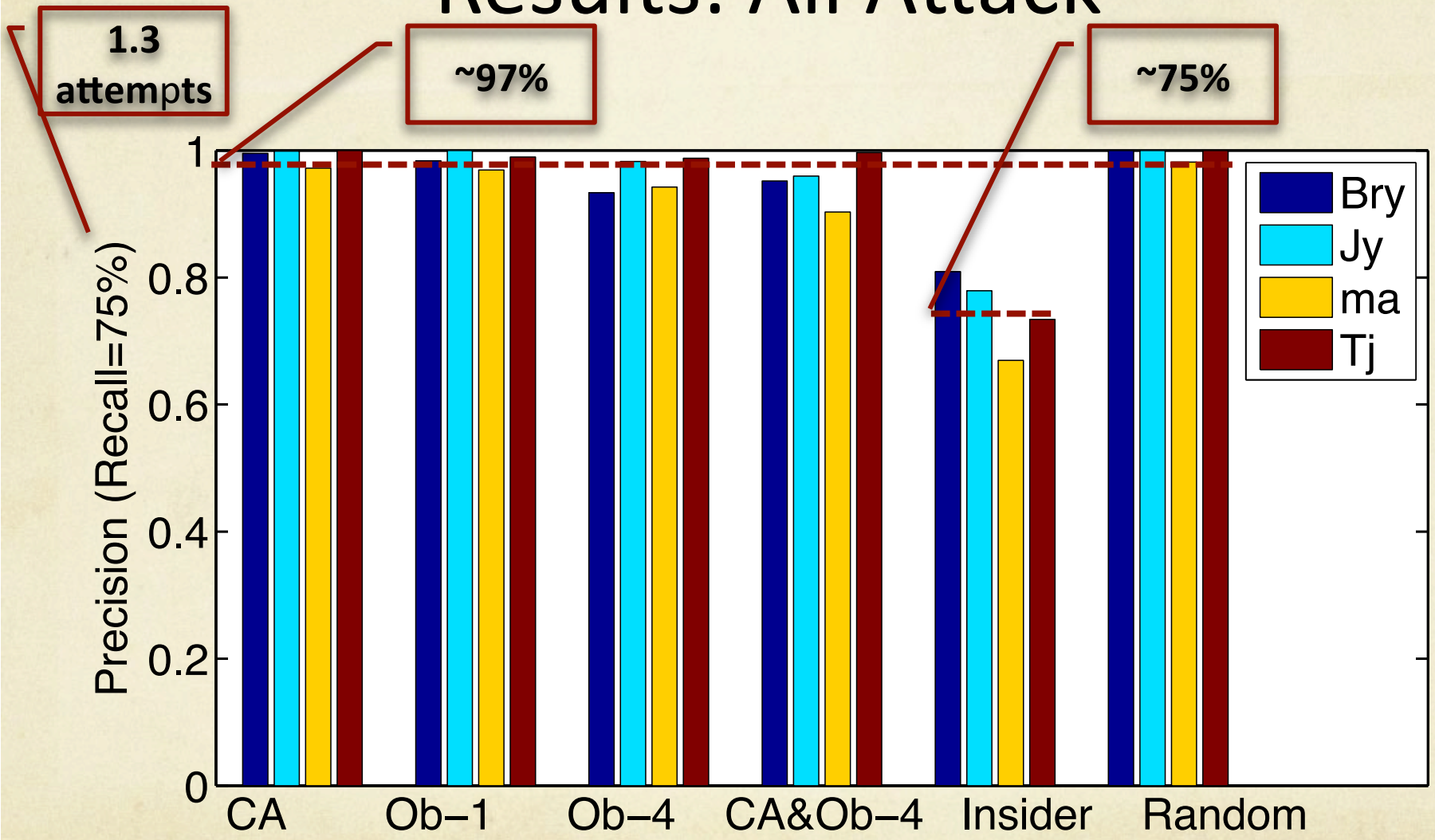
ROC Curves



Results: Legitimate User



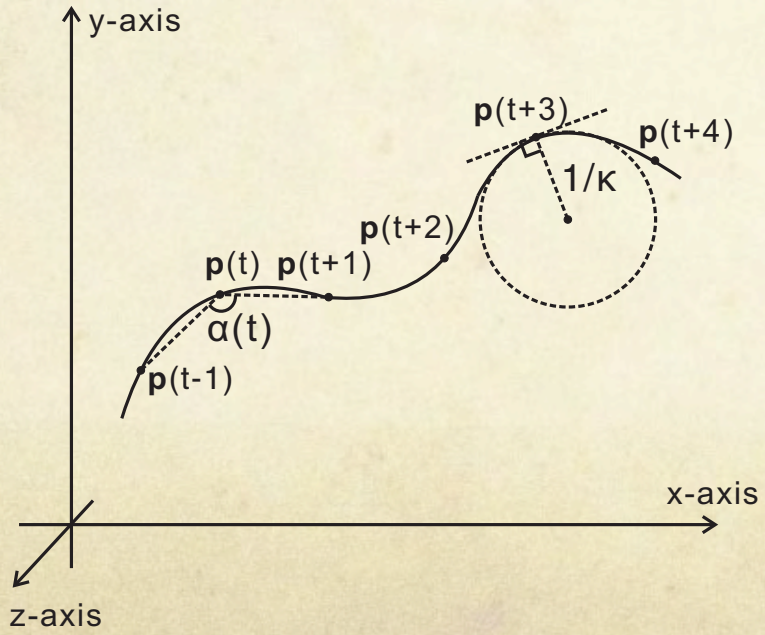
Results: All Attack



(b) Achievable precision at a 75% recall

How to Select a Feature

- We choose features based on the movements and geometries on the signature trajectories.
- Also we also learnt from the results on 2D online signature verification.



An illustration of path angle and curvature

Related Work

- This is basically a signature verification problem, which is based on research on 2D online signature.
- And also it is a behavior biometrics method, which is also related to gesture recognition and classification;
- while it is also a new way of Kinect application.

How to Select Template &Threshold

- **Template** Selection
  - The template has the minimum DTW distance to others
- **Threshold** Selection
  - Select a threshold that leads to a zero false positive rate among training samples.