浙江大学
ZHEJIANG UNIVERSITY

基于深度感知的身份认证技术

徐文渊
浙江大学

2016 阿里安全峰会

智能系统安全实验室
UBIQUITOUS SYSTEM SECURITY LAB.

Authentication

淘宝网 Taobao.com

支付宝 Alipay.com

amazon.com

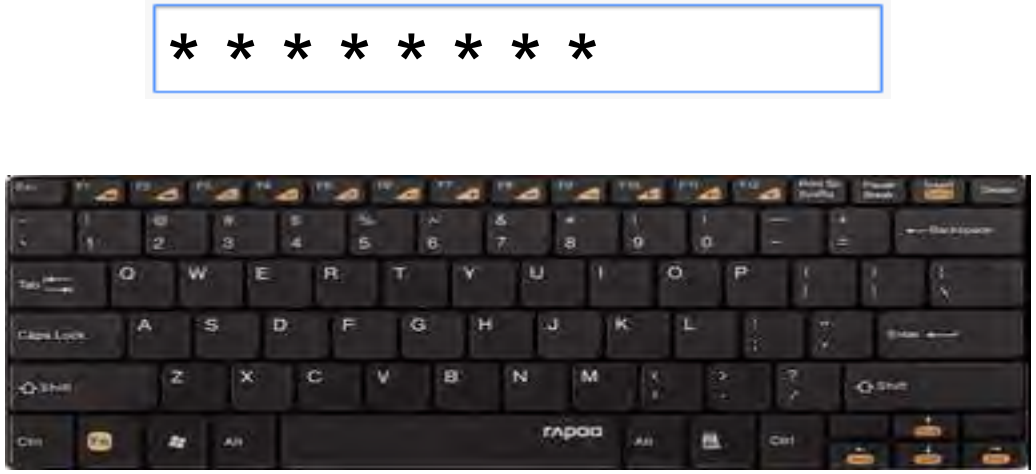
skype

Roadmap

- Passwords
- Biometrics
  - Physiological
  - Behavioral
- Behavioral Biometrics

PASSWORD

What passwords do you and your parents use?



A Large-Scale Empirical Analysis of Chinese Web Passwords, Usenix Security 2014

Password leakage

International

Sample sets： Over 100 million plaintext passwords

Share the most popular passwords

	Chinese		English	
1	123456	(2.17%)	123456	(0.88%
2	123456789	(0.65%)	12345	(0.24%
3	111111	(0.59%)	123456789	(0.23%
4	12345678	(0.39%)	Password	(0.18%
5	000000	(0.34%)	lloveyou	(0.15%

Passwords Love

	Top Chinese Pinyins	Top English Words
1	woaini (1.47%)	password (1.28%)
2	li (1.06%)	iloveyou (0.98%)
3	wang (0.97%)	love (0.76%)
4	tianya (0.89%)	angel (0.59%)
5	zhang (0.84%)	monkey (0.45%)

What is a good authentication?

- Work!
- Non – transferable
- No impersonation
- Usability

Authentication — Categories

- What you know?
  - Passwords
- What you have?
  - Keys
  - Smart cards
  - Token
- Who you are?
  - Biometrics

- Work!
- Non – transferable
- No impersonation
- Usability

BIOMETRICS

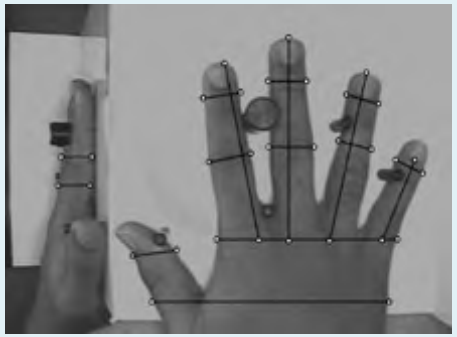
Biometrics

- Physiological→ who you are?
  - DNA, Iris, Retina, Face, Fingerprint, Finger Geometry, Hand Geometry, vein
- Behavioral→ How you act?
  - Gait, typing, mouse use characteristics, voice/speaker,

Physiological biometrics — Hand

Fingerprints

Hand Geometry



360biometrics.com

researchgate.net

Palm-print

Physiological biometrics — Vein

- Variations of Vein Recognition Technology
  - finger vein,
  - wrist vein,
  - palm vein,
  - backhand vein

Swiss startup BIOWATC

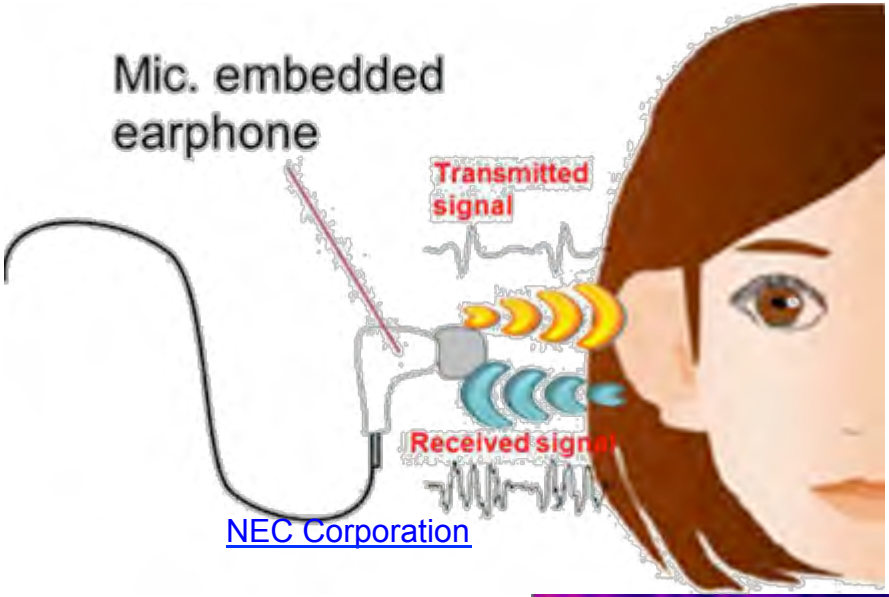
Fujitsu PalmSecure Mouse

The Hitachi Finger Vein Reader

TechSphere VP-IIX: Hand Vascular Pattern Recognit System

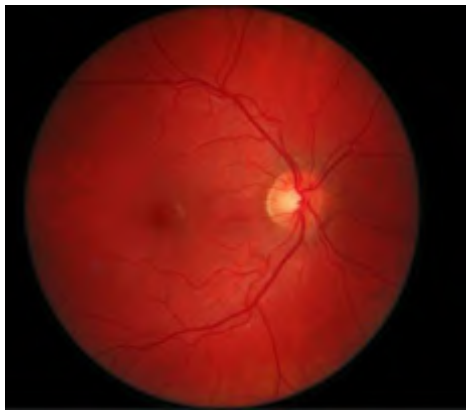
Physiological biometrics — Others

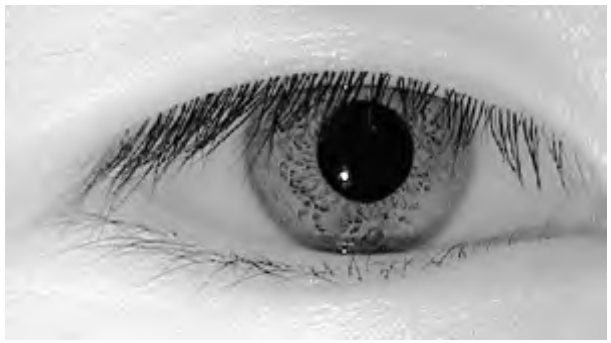
- Retina Geometry
- Iris Recognition
- Thermal Image
- Face Recognition
- DNA
- Ear Shape Recognition



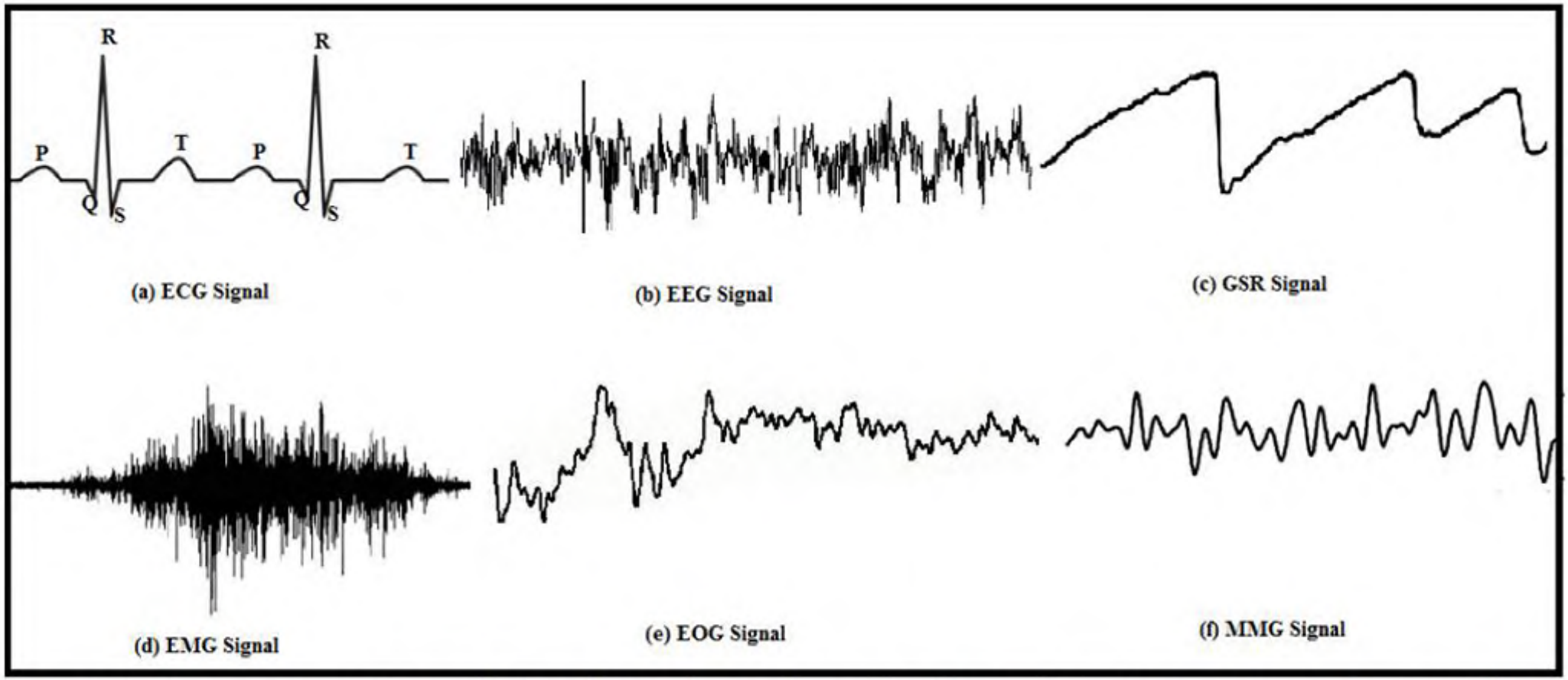
NEC Corporation


hopkinsmedicine.org


biometrics.pbworks.com



Physiological bioelectrical Signals



conventional biometric modalities, the bioelectrical signals are highly confidential and personal to an individual therefore difficult to forge.

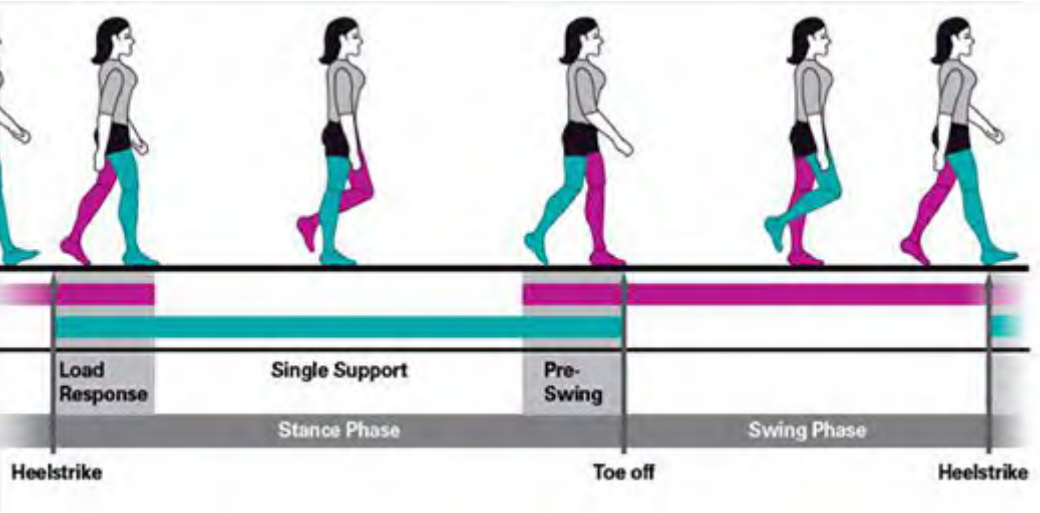
Pal, A., Gautam, A. K., & Singh, Y. N. (2015). Evaluation of Bioelectric Signals Human Recognition. Procedia Computer Science, 48, 747-753

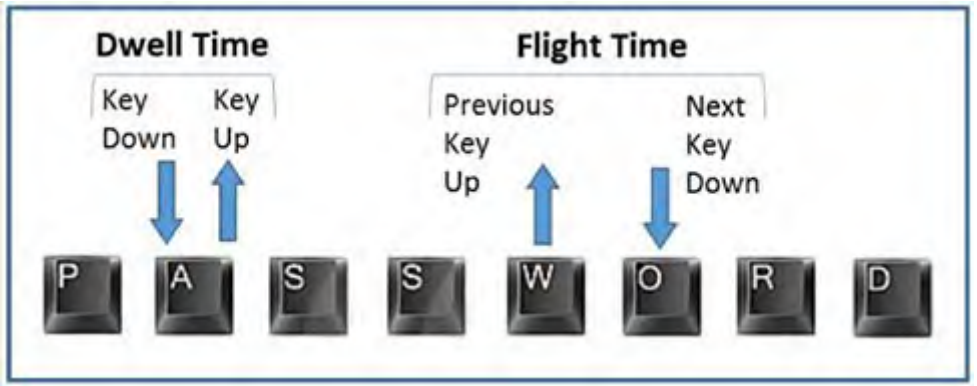
Physiological biometrics — Heartbeat

- Nymi Band -- a wearable, multi-factor authenticator
  - The band's sensor and ECG recognition algorithms monitor the shape of the wave a person's heartbeat creates.
  - Hopes you could pay with your heartbeat instead of fingerprints!

Behavioral biometrics → How you act?

- Behavioral→ How you act?
  - Gait, typing, mouse use characteristics, voice/speaker,





torialspoint.com

Biometrics - issues?


BBC Sign in News Sport Weather Shop Earth

NEWS

Home Video World Asia UK Business Tech Science Magazine

Technology

Millions of fingerprints stolen in US government hack

24 September 2015 Technology

- What does a stolen biometric mean?
- How many biometrics do you have?


USA TODAY

Five times more fingerprints were stolen in OPM hack than first estimated

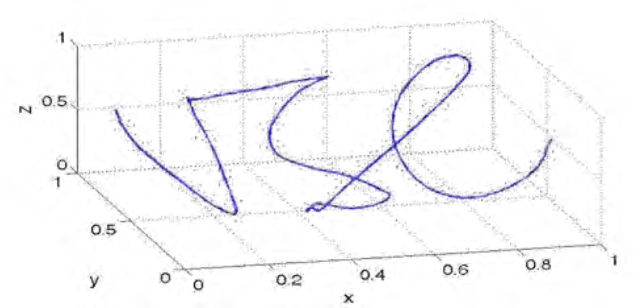
Erin Kelly, USA TODAY

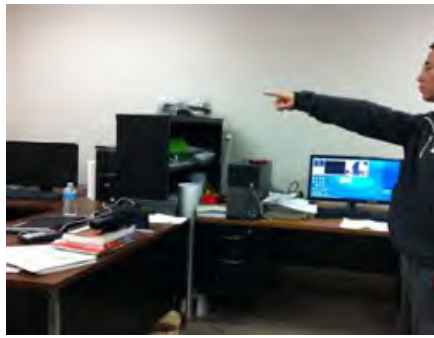
3D – SIGNATURE

J. Tian, C. Qu, W. Xu, and S. Wang, “KinWrite: Handwriting-Based Authentication Using Kinect,” in Proceedings of the 20th Annual Network & Distributed System Security Symposium (NDSS), 2013

3D-Signature

- **3D signature**: *handwriting in 3D space*
  - Write **short**, **easy to remember** passwords in the space,
    - 2 or 3 characters





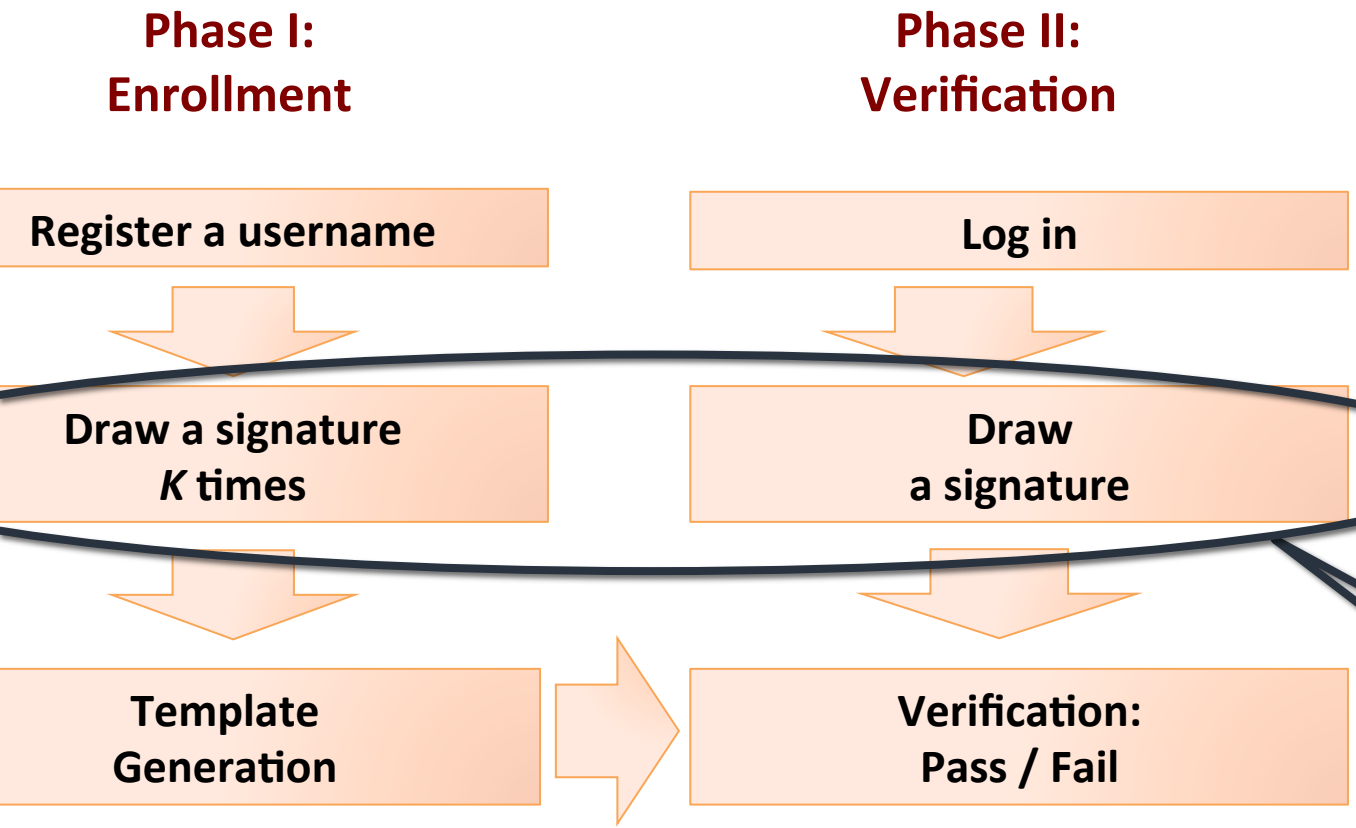
- Behavioral biometrics:
  - Can be updated
  - Difficult to duplicate
  - A weak typed password can still be strong if it is written in 3D space

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

How to capture 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



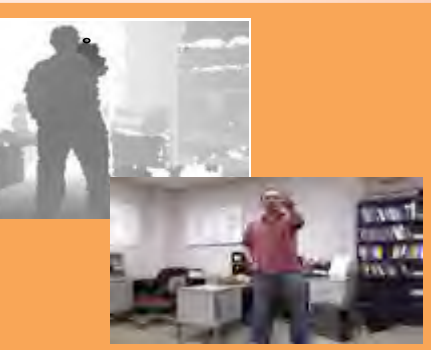
- Usability requirements
  - Rapid enrollment
  - Rapid verification
- Security requirement
  - Unforgeability

3D Signatures should be processed

KinWrite: Data Processing

Data Processing

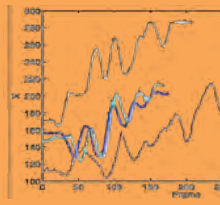
Data Acquisition



Preprocessing

Feature Extracting

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	$\log \frac{1}{\kappa(t)}$



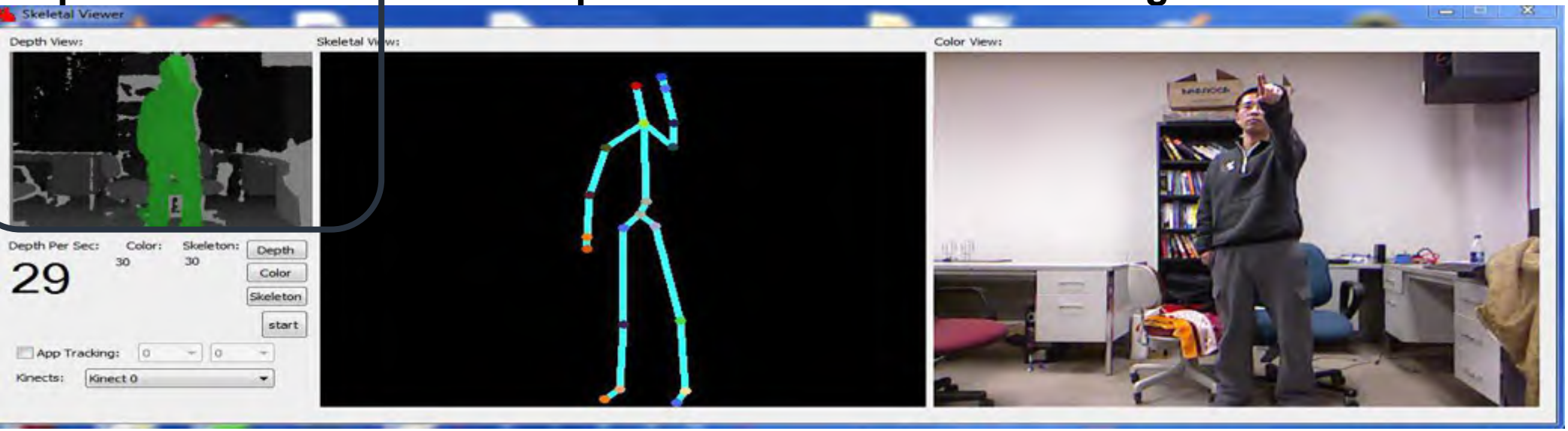
Enrollment

Verification

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**

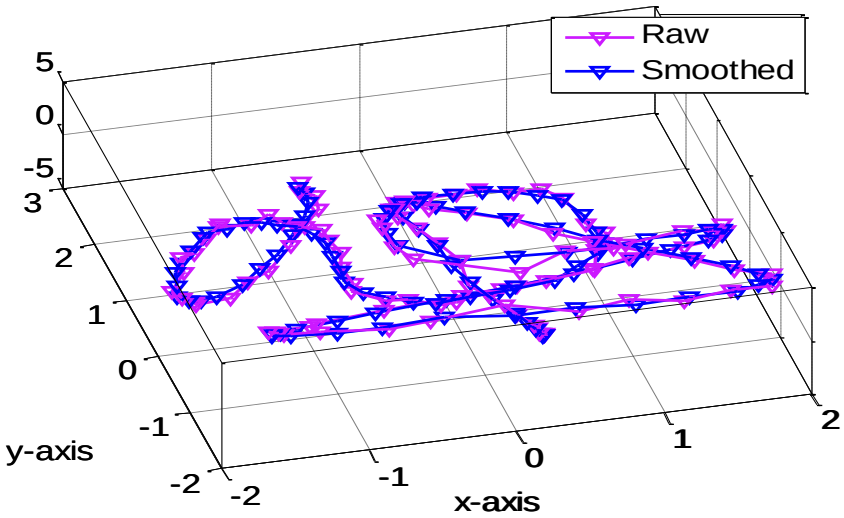


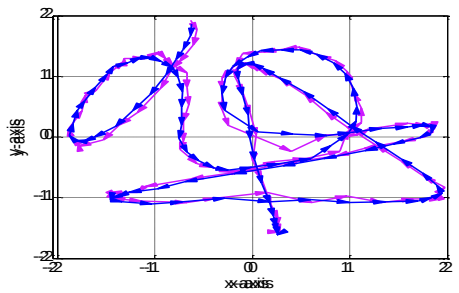
Data Acquisition → Data Preprocessing → Feature Extracting

Data processing: preprocessing

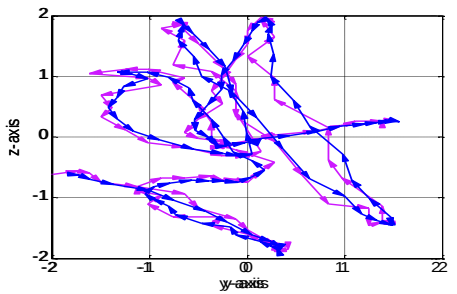
Fingertip position 1
Fingertip position 2
...
Fingertip position n

- Raw signatures
  - Noisy
- Smooth
  - Kalman filter

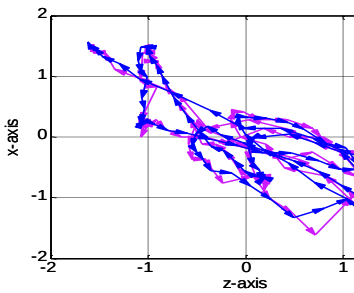




x-y plane



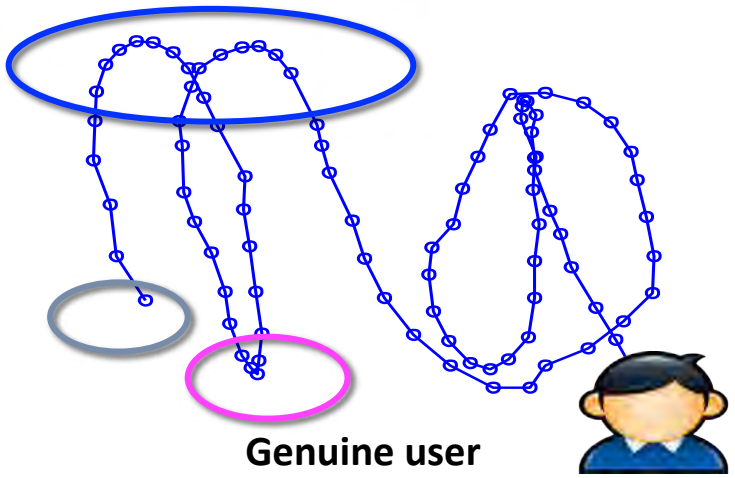
y-z plane

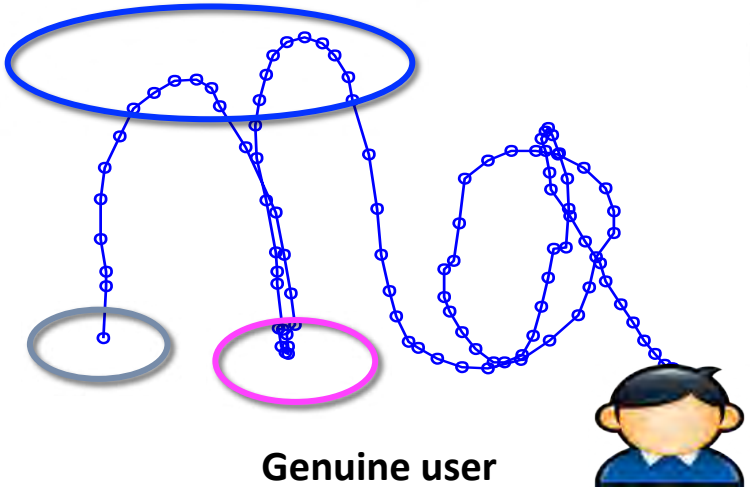


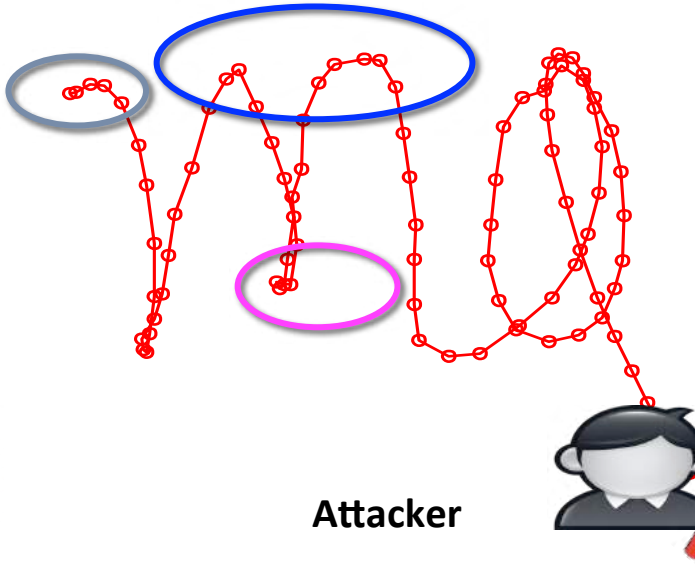
z-x plane

Data Acquisition → Data Preprocessing → Feature Extracting

Data Processing: Feature Extracting


Genuine user


Genuine user


Attacker

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*

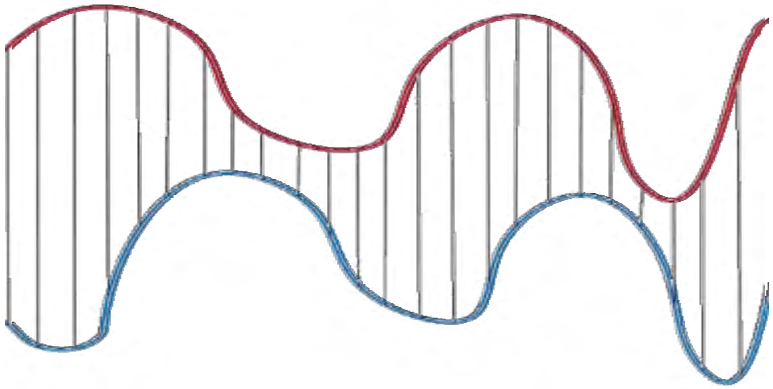
- Start point
- Turning Point
- Speed

Data Acquisition → Data Preprocessing → Feature Extracting

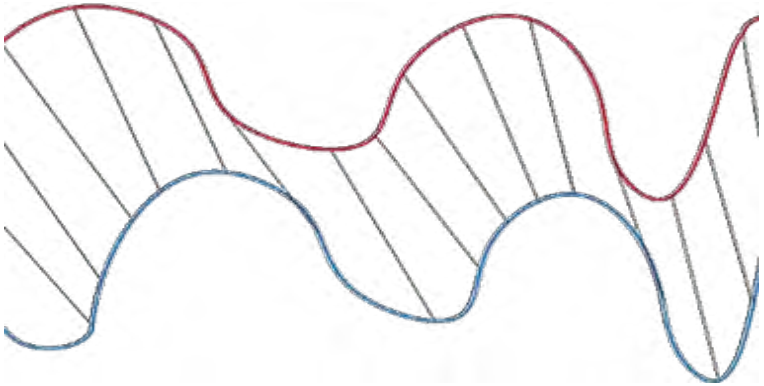
Quantify the similarity of 3D-signatures

Approach--Dynamic Time Warping (DTW)

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



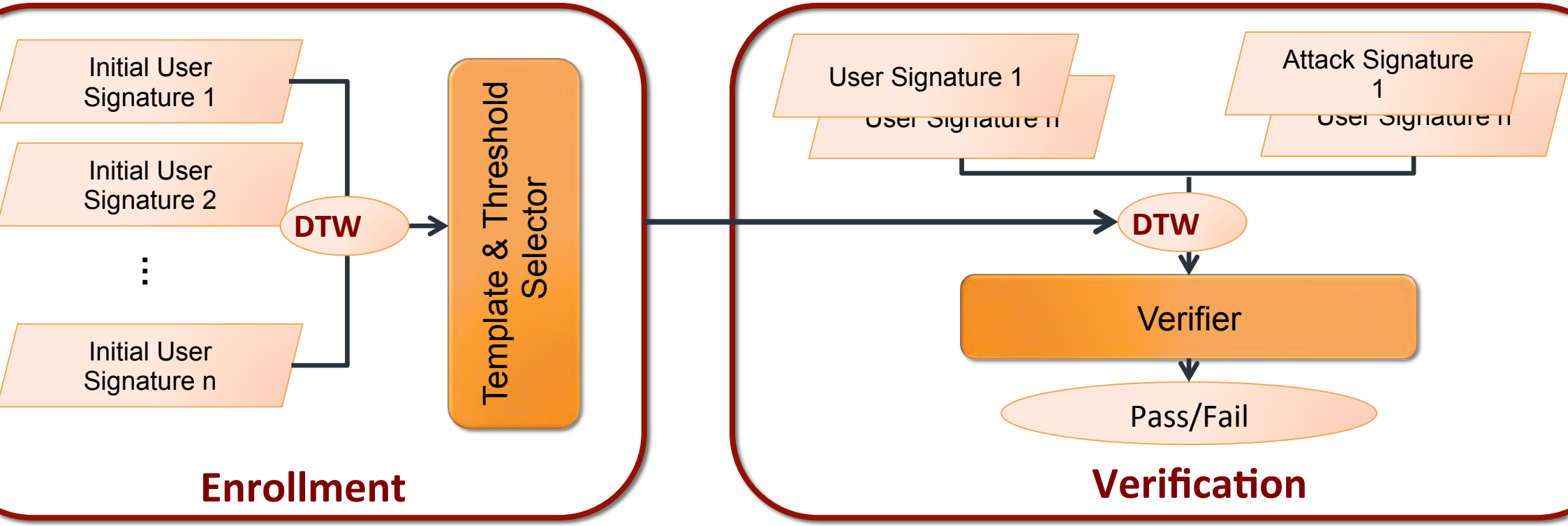
Euclidean Distance



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

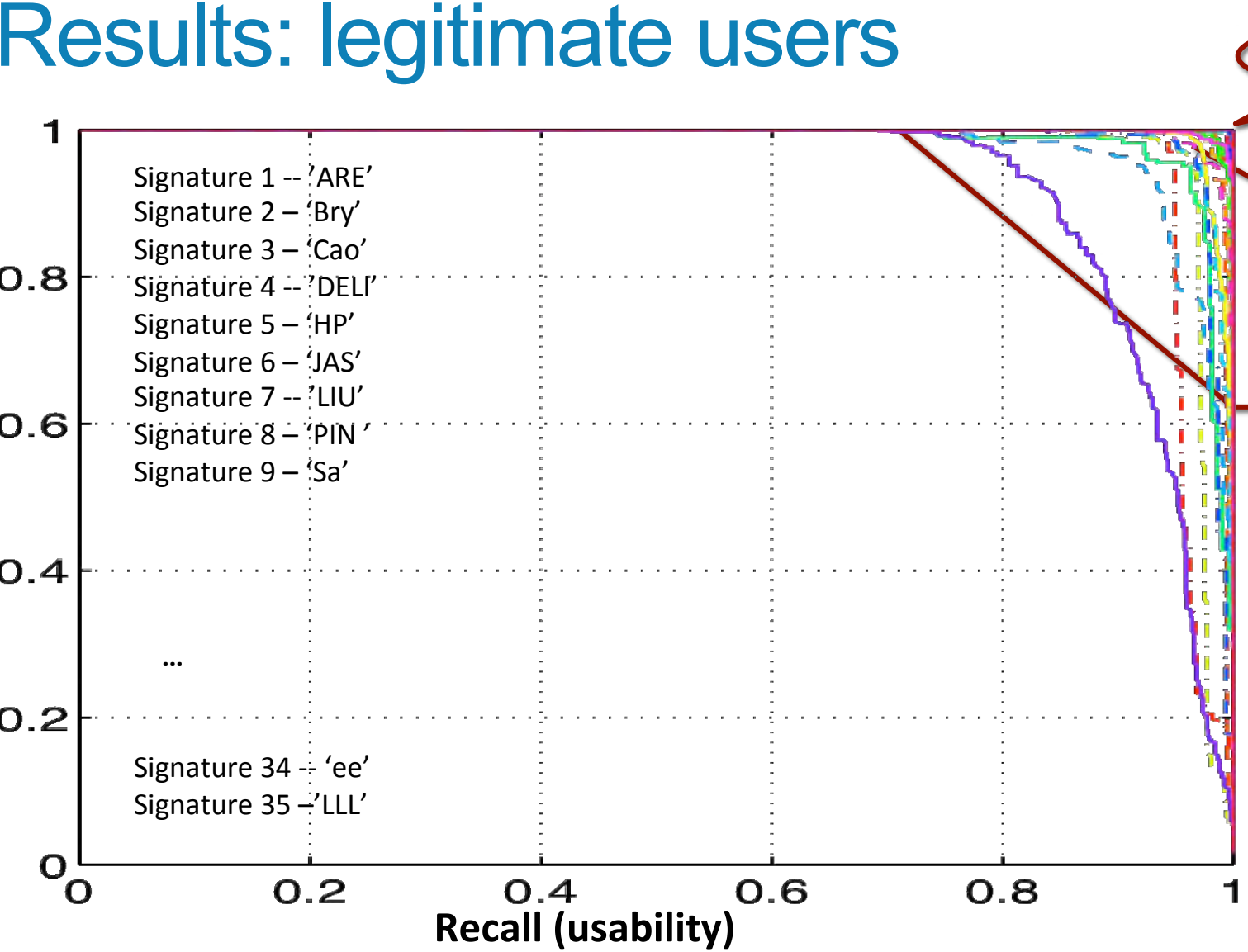
- ✧ DTW distance < threshold → pass
- ✧ DTW distance > threshold → fail to pass

Experiments: 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



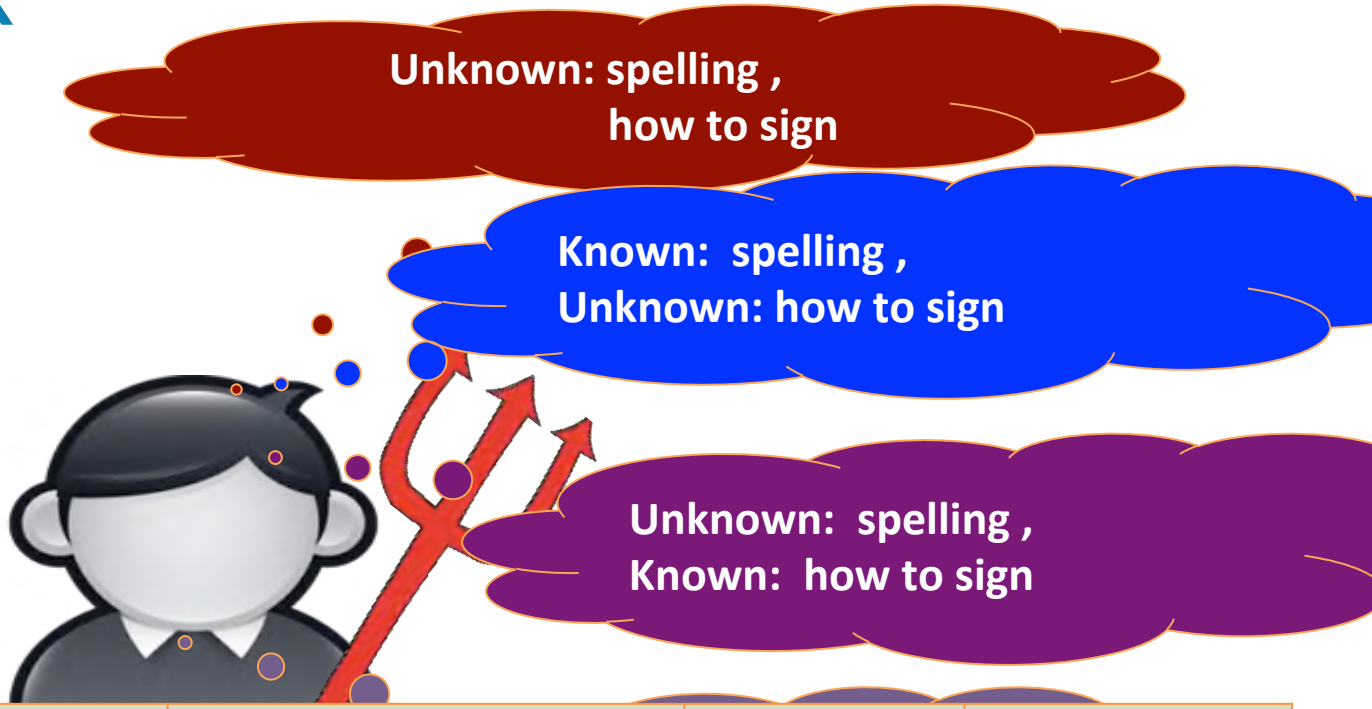
Ideal point

Most cases: >95% recall

The worst case: 70% recall

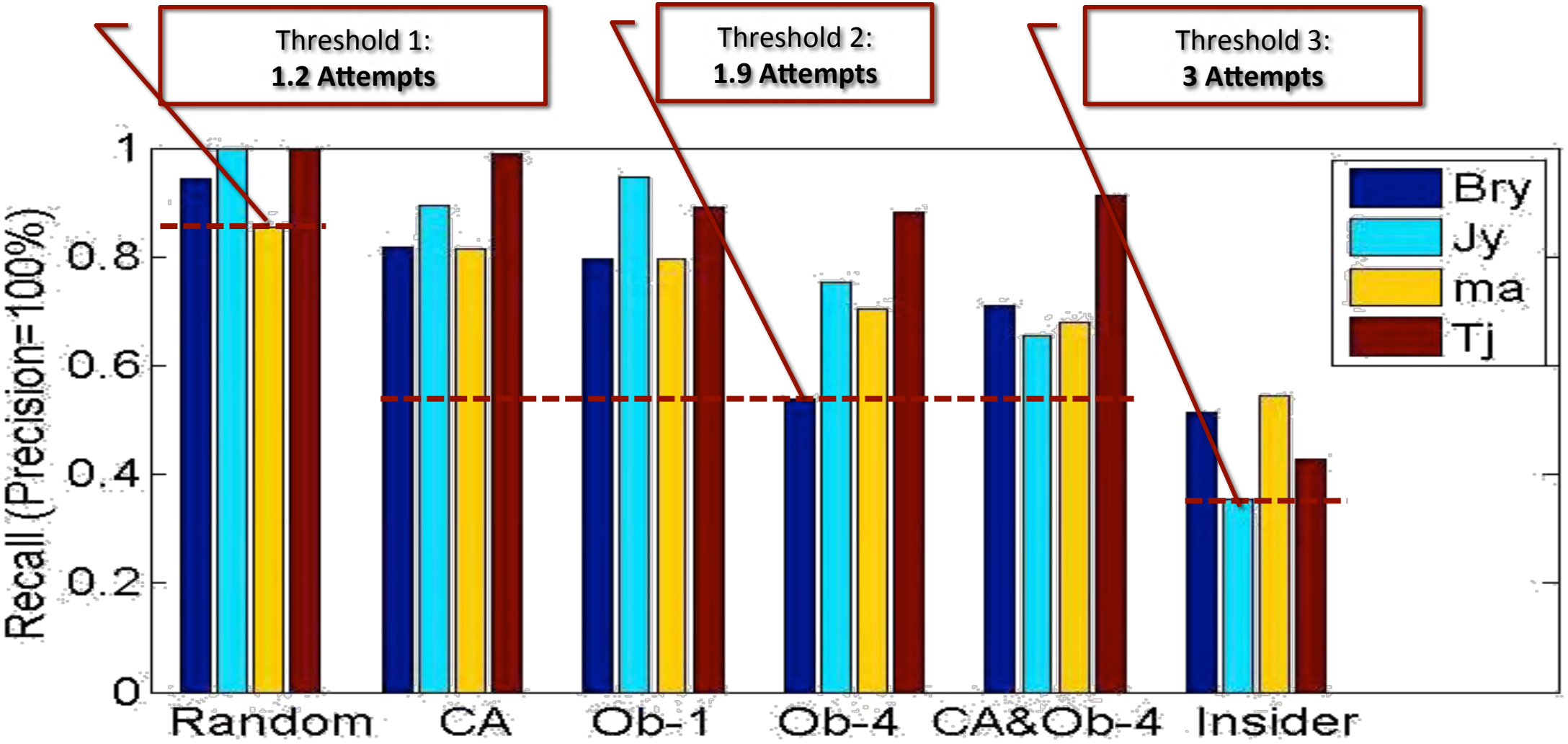
Experiments: Attack

- 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

Thank you & Questions?

ntact Information
Email: wyxu@zju.edu.cn
wyxu@cse.sc.edu
Homepage: http://www.cse.sc.edu/~wyxu