

Enhancing Mobile Device Authentication with Behavioral Biometrics

Han Gil (Paul) Jang
Washington and Lee University

Dylan Carlson
Lake Superior State University

Mengjun Xie
University of Arkansas Little Rock

Motivation

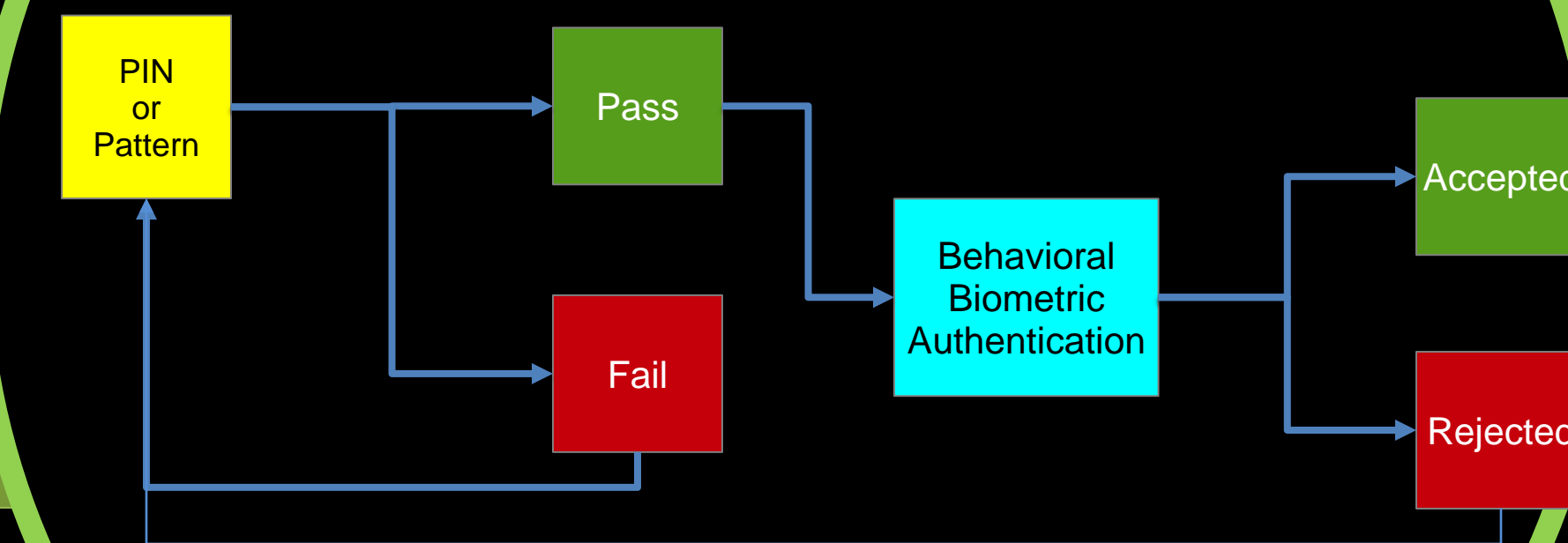
- Prevalence of mobile devices
- Weaknesses of popular authentication methods (PIN and draw patterns)
- Usability issues with current improvements on password.

Our Work

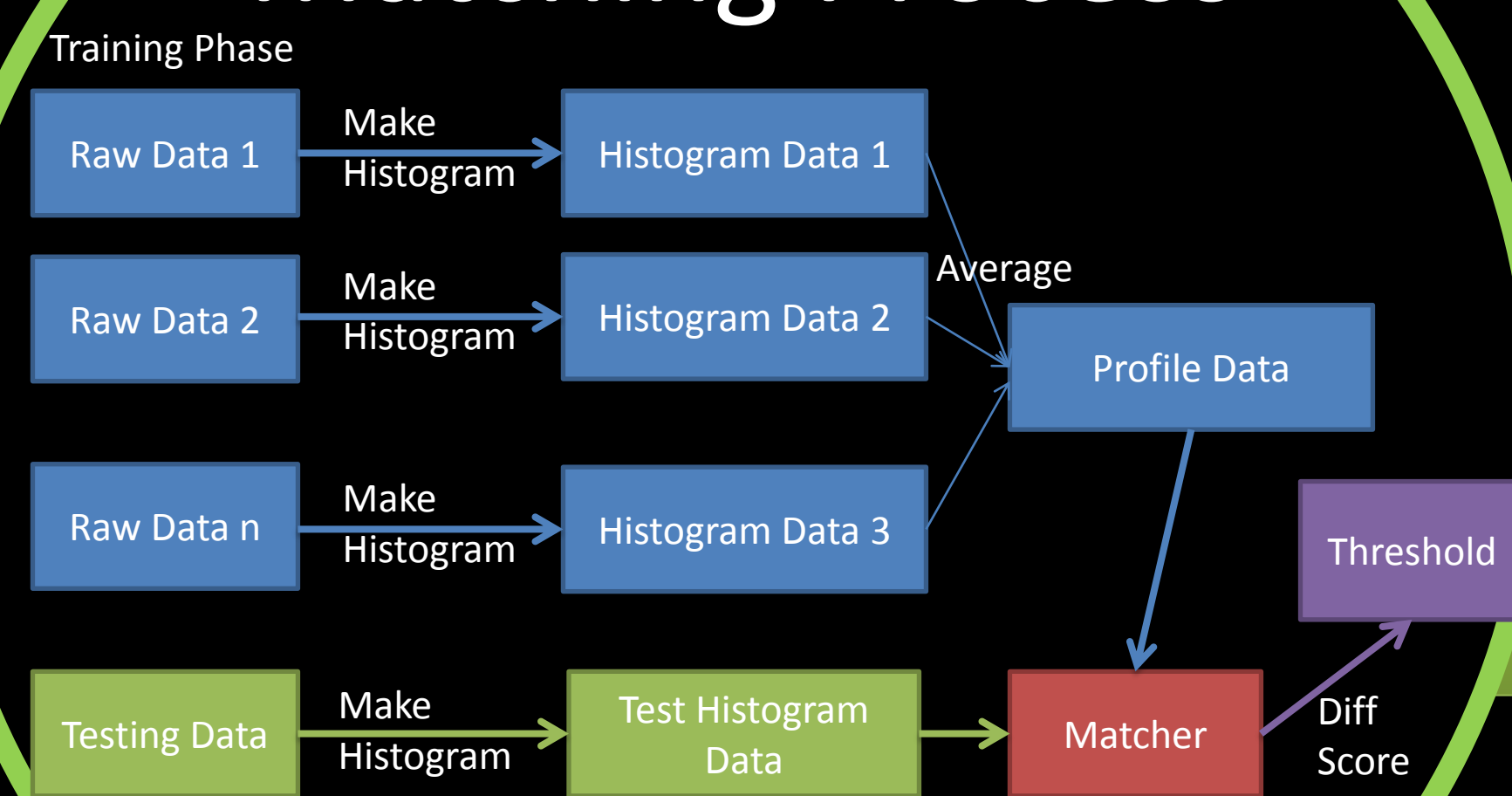
Leverage readily available behavioral biometrics to enhance authentication methods on mobile devices.

- Our approach does
- Not affect usability
 - Not require additional hardware
 - Provide another authentication factor

Authentication Process



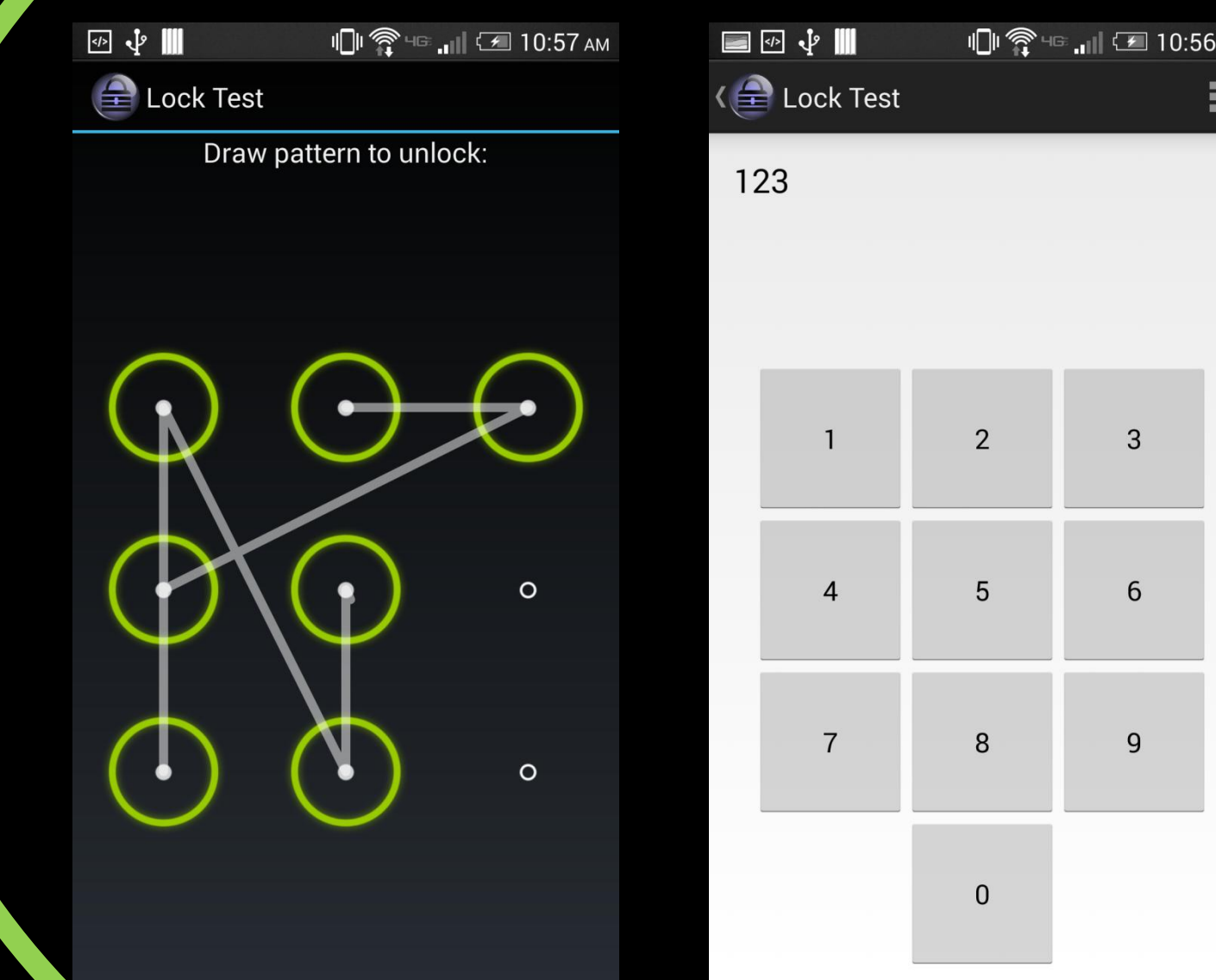
Matching Process



Collected Features

- X,Y coordinates
- Pressure
- Area
- Acceleration
- Angular acceleration
- Pass/Fail
- Distance
- Angle
- Derivatives of features

Data Collection



Results (I)

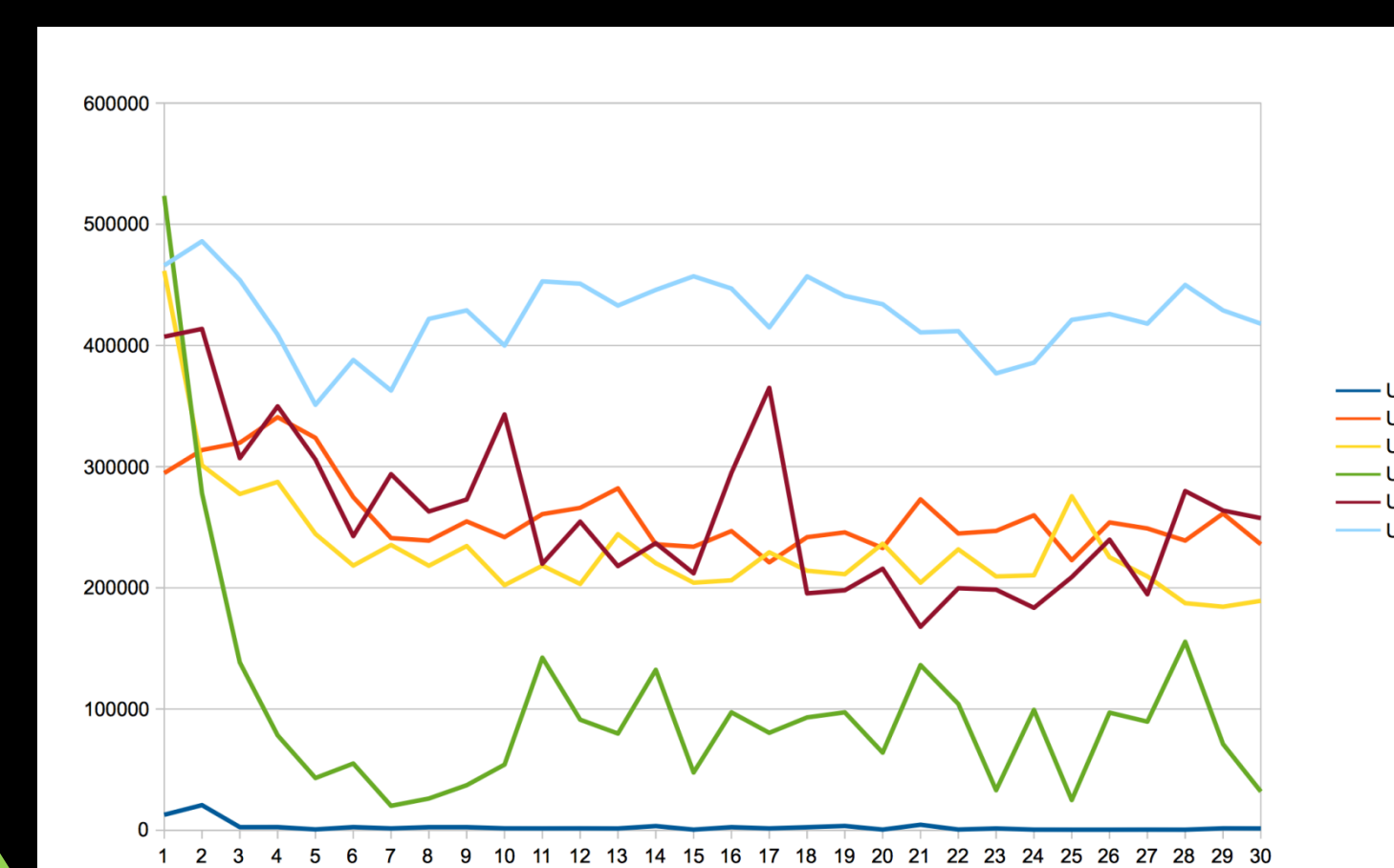
FAR rate (with 10% FRR)
of Users: 16, # of test samples: 30

- | | |
|--------------------------|--------------------------|
| Phone Session 1: | Phone Session 2: |
| • Simple Pattern: 7.68% | • Simple Pattern: 7.86% |
| • Complex Pattern: 6.20% | • Complex Pattern: 8.79% |
| • Simple Pin: 12.77% | • Simple Pin: 8.94% |
| • Complex Pin: 5.77% | • Complex Pin: 9.13% |

- Tablet Session 3:**
- Simple Pattern: 8.86%
 - Complex Pattern: 5.98%
 - Simple Pin: 3.89%
 - Complex Pin: 2.12%

Results (II)

Difference score for each attempt



Conclusion

1. Our approach currently achieves EER (equal error rate) of less than 10% and in many cases lower than 5%.
2. Enhancing user authentication with behavioral biometrics is very promising.
3. Improvements can be made by
 - Tuning the parameters for feature processing and comparison.
 - Pruning and adding to the current feature set.

Acknowledgment:
NSF CyberSAFE@UALR REU Site
(Award #: CNS-1359323)