Exploring Games for Improved Touchscreen Authentication on Mobile Devices

Padmaja Scindia

pscindia@nyit.edu

Jonathan Voris

jvoris@nyit.edu

New York Institute of Technology

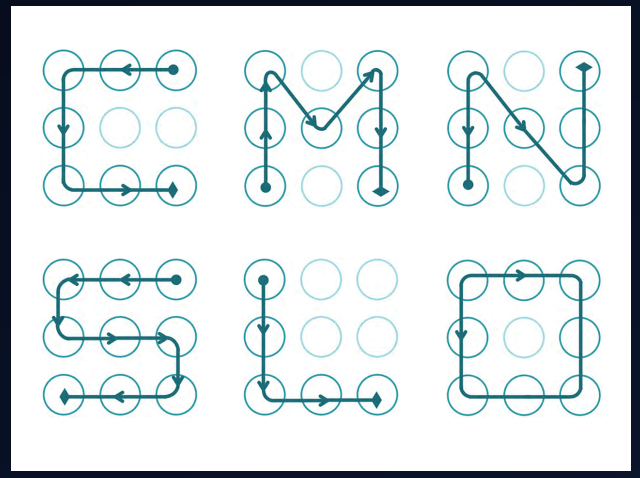
Department of Computer Science

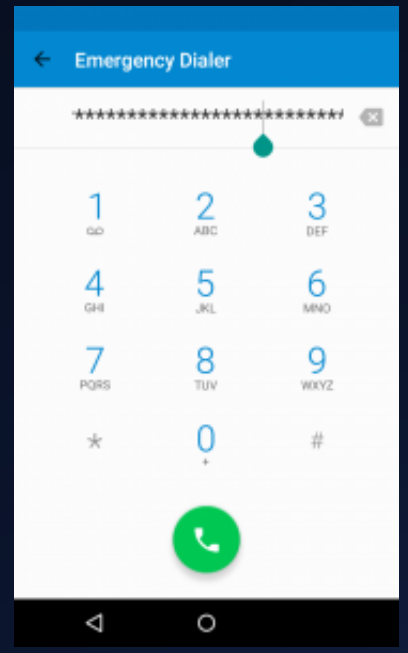
Mobile Devices Need Strong Authentication

- Mobile devices increasingly responsible for sensitive information
- Their form factor makes them easily stolen
  - 3.1 million devices stolen in 2013 [8]
- Data loss from mobile devices ranked the largest threat to mobile computing [4]

Mobile User Authentication is Not Easy

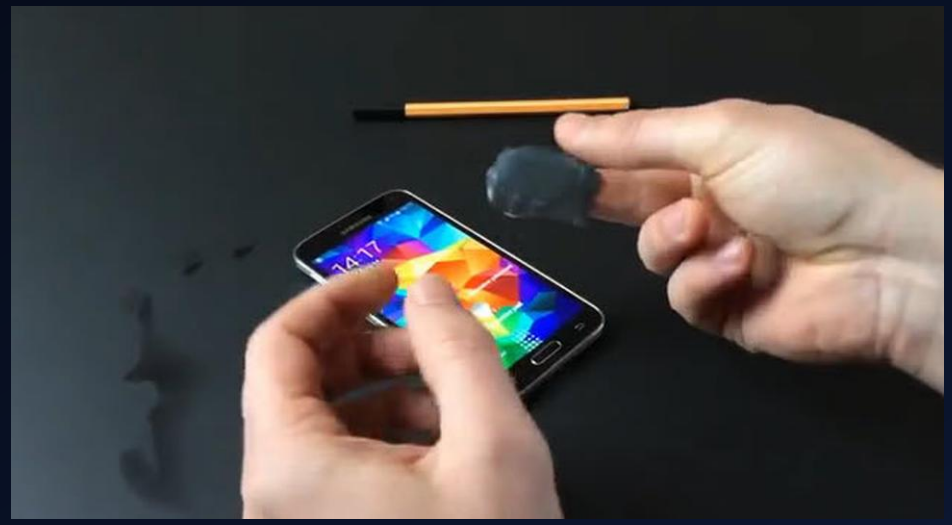
- Mobile authentication is vulnerable to observation attacks [6]
- Usability concerns prevent adoption of existing methods
- 47% of smartphone owners don’t use a PIN, password, or unlock pattern [8]
- 34% take no security precautions with their mobile devices [8]
- Solutions must be resource efficient





Biometrics to the Rescue?

- Devices can verify user identity by measuring distinctive characteristics
- Traditional biometrics measure physical traits
- Advantages:
  - Not vulnerable to observation
  - Harder to lose
- Disadvantages:
  - Requires specialized hardware
  - Usability issues
  - Only performed at session start



Behavioral Biometrics

- Can users be authenticated based on the manner in which they use a device?
- Improves usability
  - Natural device usage
- Active authentication for improved security
  - Verify identity throughout a session
- Potential modalities:
  - Stylometry [1]
  - Application usage [5]
  - Device movement [7]
  - Touchscreen dynamics [9]

Behavioral Biometrics

- Challenges:
  - Small resource footprint
  - Privacy consciousness
  - Detection time
  - Modality relevance

Idea: Use Gameplay for Authentication

- Can users be authenticated by how they play a game?
  - Are a person's gameplay habits consistent?
  - Degree of variation between users?
- Why games?
  - Natural usability benefits [2][3]
  - Widespread popularity
  - Privacy friendly
  - Encourage rapid and distinct input

A (Very) Preliminary Evaluation

- Developed a touchscreen input sensor for Android
- Installed on a Samsung Galaxy along with 3 popular games:
  - Angry Birds
  - Flow Free
  - Fruit Ninja
- Conducted IRB approved study with 12 participants
  - Played each game for 5 minutes

Gameplay Analysis

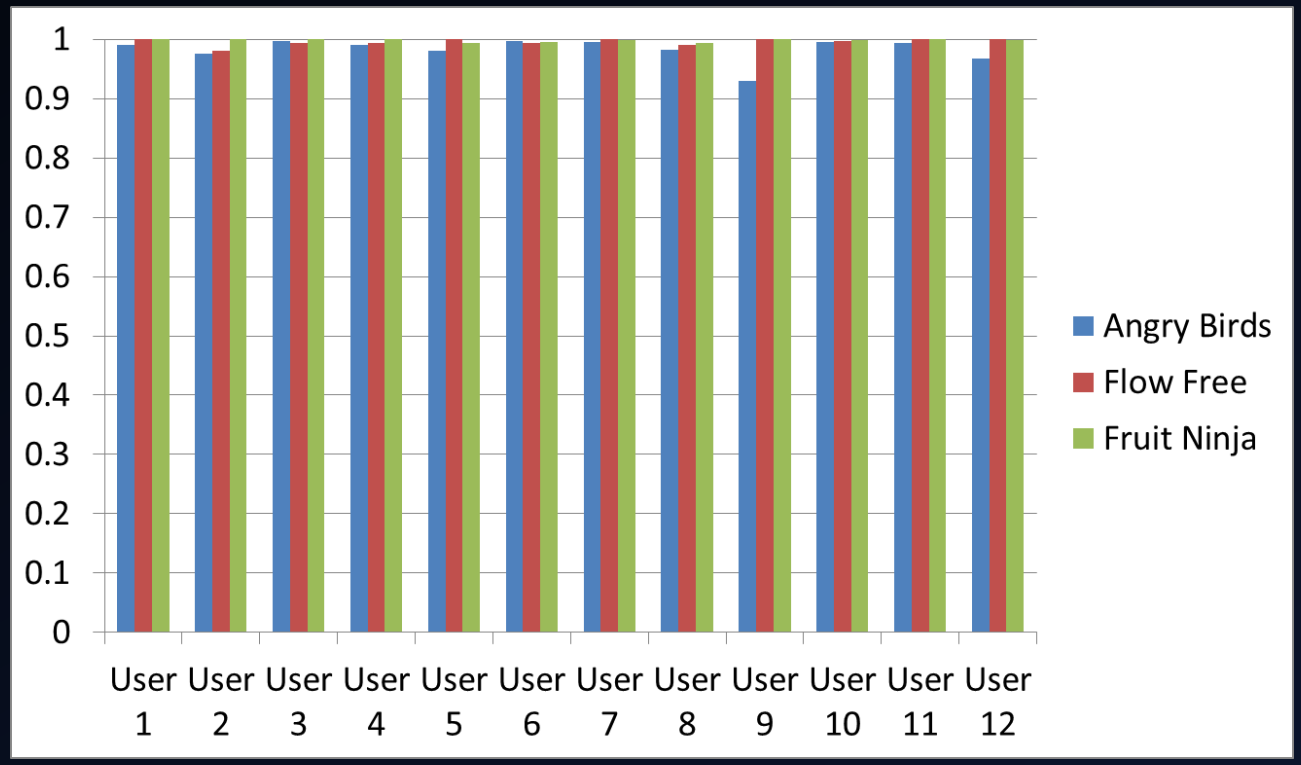
- Randomly selected 300 distinct gestures per user per game
- Derived 17 properties of touchscreen interactions:

1) Initial X coordinate
2) Initial Y coordinate
3) Final X coordinate
4) Final Y coordinate
5) Pressure
6) Area covered
7) Finger width
8) Gesture length along X axis
9) Gesture length along Y axis
10) Distance
11) Direction
12) Speed along X axis
13) Speed along Y axis
14) Speed along trajectory
15) Velocity
16) Angular velocity
17) Finger orientation

- Applied a Support Vector Machine to gesture features per game
  - Trained with Sequential Minimal Optimization
  - Tested with 10-fold cross validation

Results

Game	TP Rate	FP Rate	Precision	AUC
Angry Birds	92.17%	0.70%	92.41%	0.983
Flow Free	98.86%	0.10%	98.87%	0.996
Fruit Ninja	99.45%	0.05%	99.46%	0.998



Area Under the ROC Curve for each Combination of User and Game

Conclusion

- Behavioral biometrics are a promising approach to mobile authentication
- Users can potentially be authenticated by how they play touchscreen games
- Further research planned into how games impact authentication usability and speed
- Future work:
  - More comprehensive study
  - Comparison of a wider variety of application usage
  - Susceptibility of gameplay to attack (observation, mimicry, etc.)

Thank you!

References

[1] L. Fridman, S. Weber, R. Greenstadt, and M. Kam. “Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location” IEEE Systems Journal, 2015.

[2] A. Gallego, N. Saxena, and J. Voris. “Exploring Extrinsic Motivation for Better Security: A Usability Study of Scoring-Enhanced Device Pairing.” In Financial Cryptography and Data Security, 2013.

[3] R. Halprin and M. Naor. “Games for Extracting Randomness.” In Proceedings of the 5th Symposium on Usable Privacy and Security, 2009.

[4] P. Ruggiero and J. Foote. “Cyber Threats to Mobile Phones.” United States Computer Emergency Readiness Team Report. Available at: https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf, 2011.

[5] M. B. Salem, J. Voris, and S. Stolfo. “Decoy Applications for Continuous Authentication on Mobile Devices.” In 1st Who Are You?! Adventures in Authentication Workshop (WAY) co-located with the 10th Symposium on Usable Privacy and Security (SOUPS), 2014.

[6] F. Schaub, R. Deyhle, and M. Weber. “Password entry usability and shoulder surfing susceptibility on different smartphone platforms.” In Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia, 2012.

[7] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. Balagani. “HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users.” IEEE Transactions on Information Forensics and Security, 2016.

[8] D. Tapellini. “Smart Phone Thefts Rose to 3.1 Million Last Year, Consumer Reports Finds.” Available at: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm, 2014.

[9] H. Xu, Y. Zhou, and M. R. Lyu. “Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones.” In Symposium On Usable Privacy and Security (SOUPS), 2014.