Biometric User Authentication on Mobile Devices through Gameplay

REU fellow: Kirsten Giesbrecht[1], Faculty mentor: Dr. Jonathan Voris[2]

Affiliation: 1.Centre College 2. School of Engineering and Computing Sciences, NYIT

NYIT Research Experience for Undergraduates (REU)

May 26 – July 30, 2015

NYIT School of Engineering and Computing Sciences

User Authentication

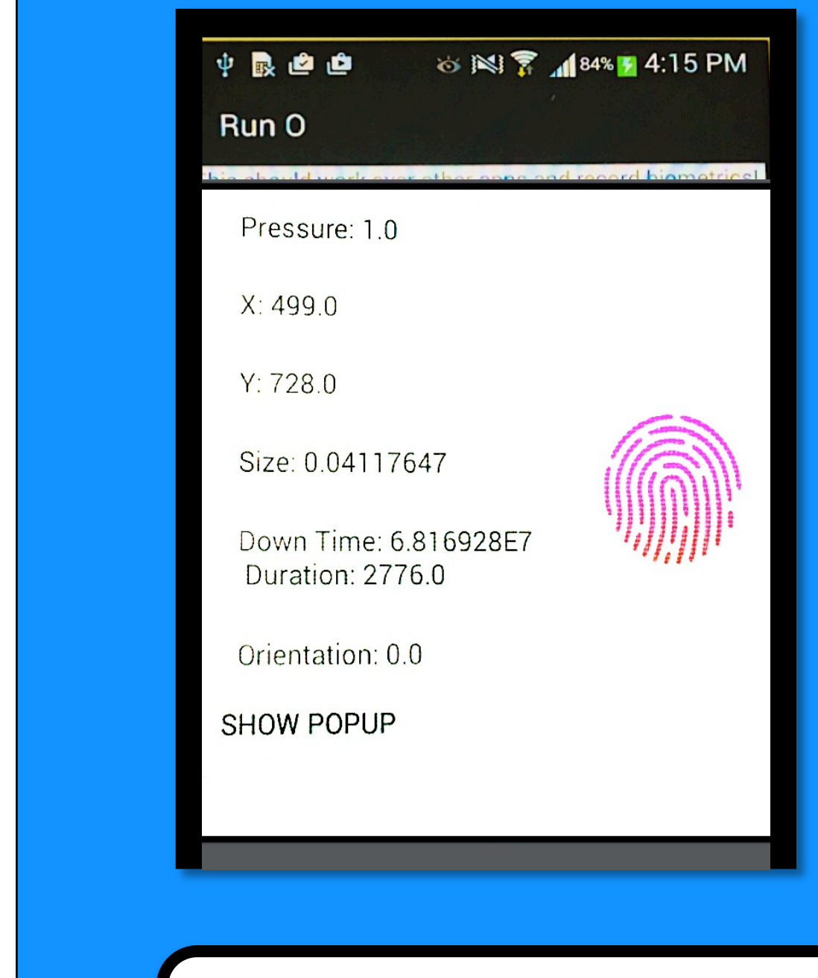
- **Alphanumeric Passcodes**
  - Easily Forgotten
- **Visual Passcodes**
  - Smudge Attacks or Shoulder Surfing
- **Biometric Features**
  - Physical- fingerprints
  - Behavioral- pressure, location, duration of touch
  - Difficult to replicate, used for identification
- **Related Research**:
  - 77% accuracy in a long-term study using a visual password pattern
  - 100% accuracy in authenticating smartphone owner after 6 swipes in another study
  - Users identified through gameplay using biometric features extracted from mouse clicks on desktop computers
- **Biometric features extracted through gameplay on touch screens of mobile devices for user authentication has not been tested**

Methods

- **The researchers propose designing a short game users play to unlock a smartphone, replacing passcodes.**
- **Passively authorize users from biometric features extracted from:**
  - Swipe or Tap
- **Extracting features:**
  - Initial time/ duration
  - Pressure
  - Size
  - location (x,y)
  - Major axis

- Testing on rooted Samsung Galaxy S III and Motorola Moto G.

1. Application written in Android Studio is used to display biometric features from touch operations within App (Fig. A)



Run O

Pressure: 1.0

X: 499.0

Y: 728.0

Size: 0.04117647

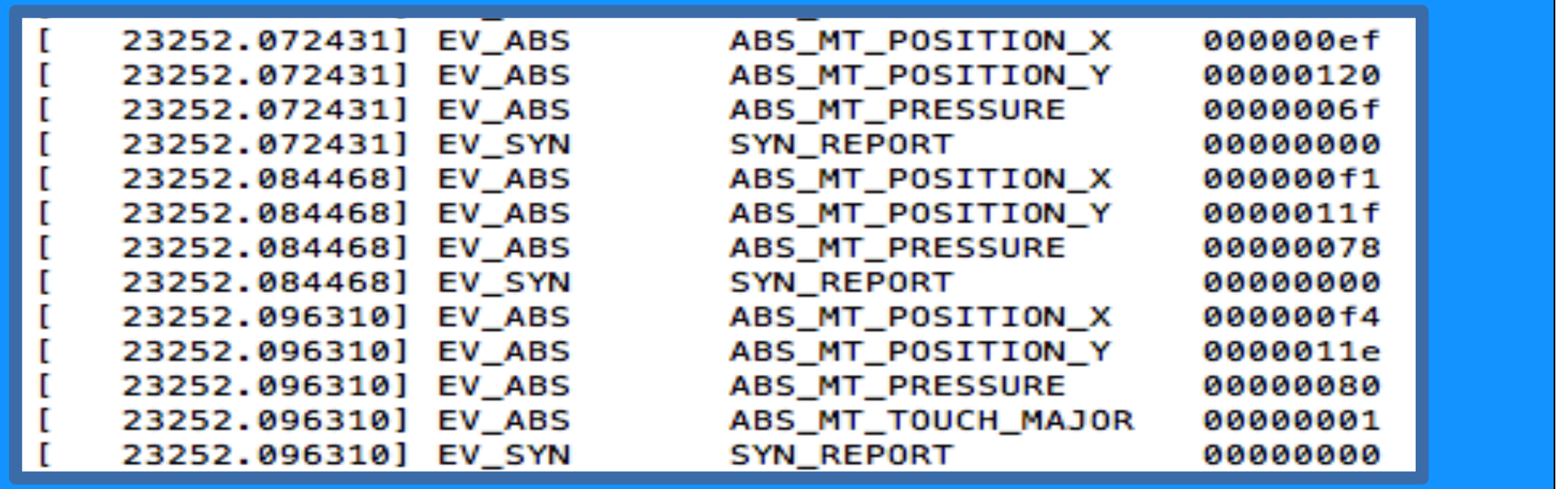
Down Time: 6.816928E7
Duration: 2776.0

Orientation: 0.0

SHOW POPUP

Figure A. Application displays biometric features extracted from touch operations

2. Background application written for rooted phones writes a file of recorded biometric features from touch data as the user operates the mobile device (Fig. B)



```
[    23252.072431] EV_ABS          ABS_MT_POSITION_X     000000ef
[    23252.072431] EV_ABS          ABS_MT_POSITION_Y     00000120
[    23252.072431] EV_ABS          ABS_MT_PRESSURE       0000006f
[    23252.072431] EV_SYN          SYN_REPORT            00000000
[    23252.084468] EV_ABS          ABS_MT_POSITION_X     000000f1
[    23252.084468] EV_ABS          ABS_MT_POSITION_Y     0000011f
[    23252.084468] EV_ABS          ABS_MT_PRESSURE       00000078
[    23252.084468] EV_SYN          SYN_REPORT            00000000
[    23252.096310] EV_ABS          ABS_MT_POSITION_X     000000f4
[    23252.096310] EV_ABS          ABS_MT_POSITION_Y     0000011e
[    23252.096310] EV_ABS          ABS_MT_PRESSURE       00000080
[    23252.096310] EV_ABS          ABS_MT_TOUCH_MAJOR    00000001
[    23252.096310] EV_SYN          SYN_REPORT            00000000
```

Figure B. Portion of file written by the background application containing biometric features extracted a user while plays Flappy Bird on Motorola Moto G.

3. Six games from the Google Play store are selected to be tested (Table 1, Fig. C)

Game	Action
Temple Run	Swipe, tilt phone
Fruit Ninja	Swipe
Angry Birds	Swipe, drag
Flow Free	Swipe, drag
Candy Crush	Swipe
Flappy Bird	Tap

Table 1. Games available on the Google Play store are tested to investigate if they serve as reliable methods for extracted reliable and unique biometric features

4. Researchers are testing the games, playing each game for 15 minutes as the background application records biometric features and writes the file

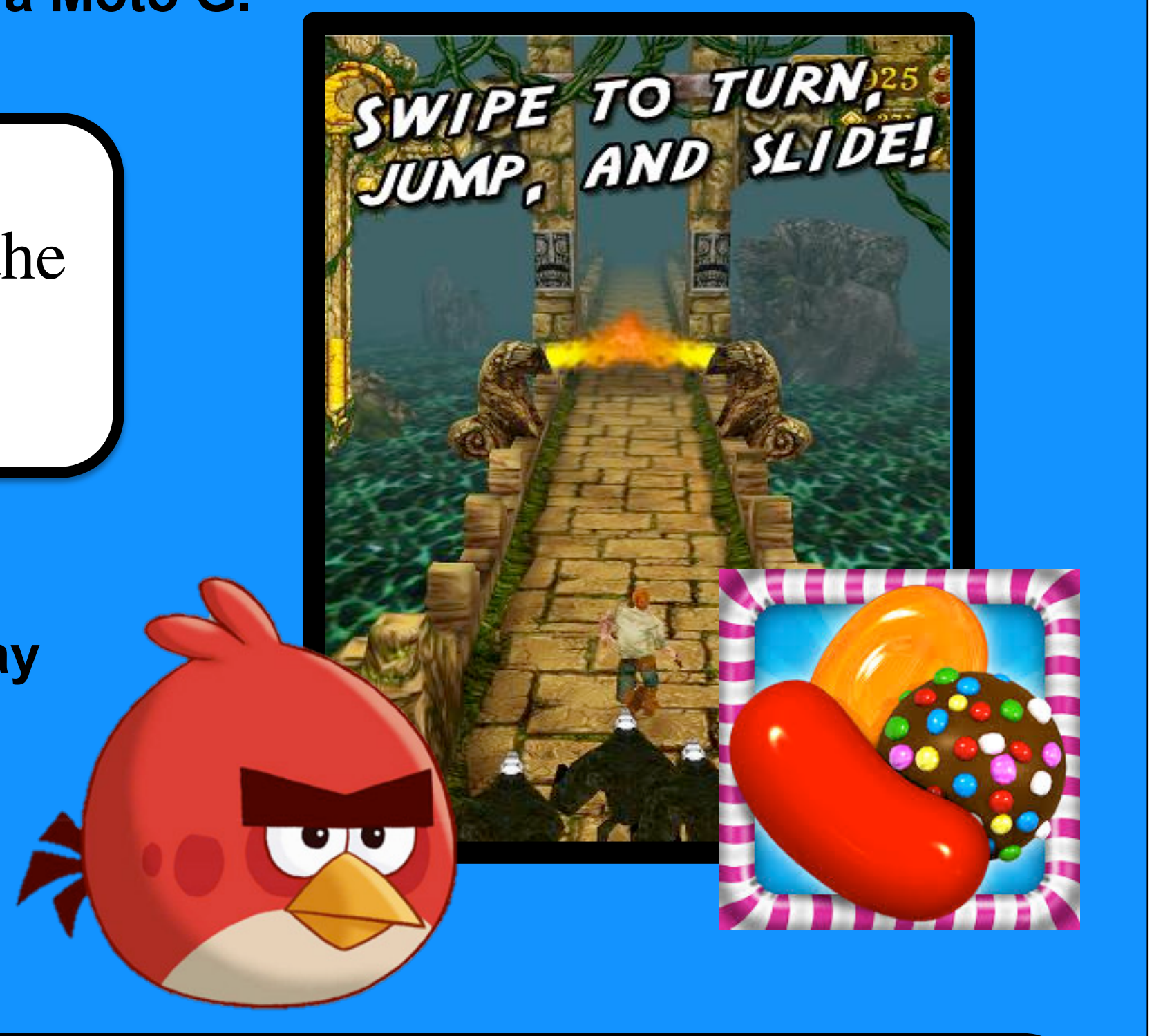
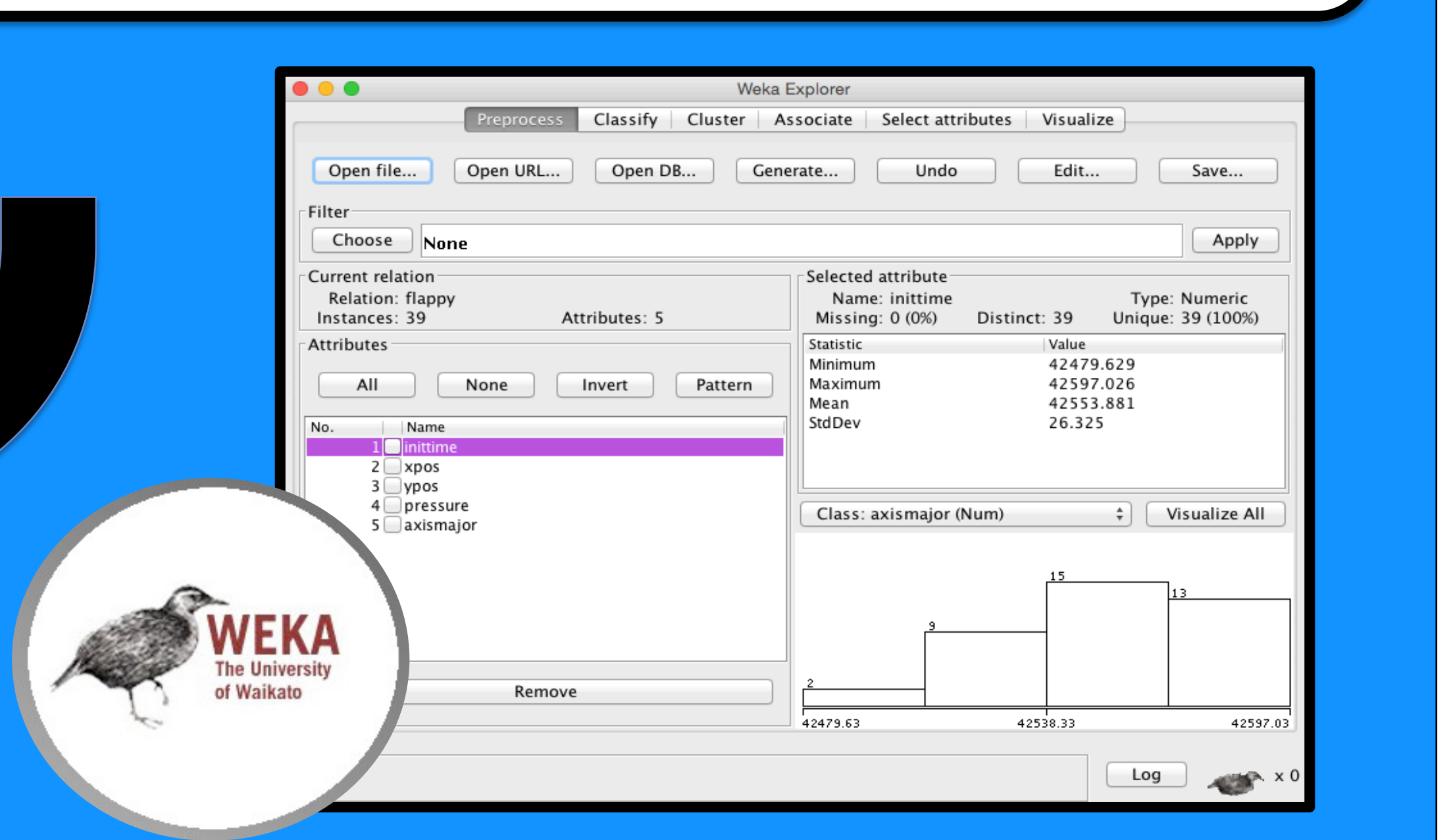


Figure C. Candy Crush, Angry Birds, and Temple Run are tested from the Google Play store. The new game may consist of simple movements similar to these games

5. The data collected will be analyzed in Weka. If the results indicate that the features are a reliable form of identification, a new game will be created (Fig. D)



Weka Explorer

Preprocess | Classify | Cluster | Associate | Select attributes | Visualize

Open file... | Open URL... | Open DB... | Generate... | Undo | Edit... | Save...

Filter: Choose None Apply

Current relation
Relation: flappy
Instances: 39   Attributes: 5

Attributes: All | None | Invert | Pattern

No.	Name
1	inittime
2	xpos
3	ypos
4	pressure
5	axismajor

Remove

Selected attribute
Name: inittime   Type: Numeric
Missing: 0 (0%)   Distinct: 39   Unique: 39 (100%)

Statistic	Value
Minimum	42479.629
Maximum	42597.026
Mean	42553.881
StdDev	26.325

Class: axismajor (Num)   Visualize All

Log

Figure D. Example of data to be analyzed in Weka

6. The new game will be inserted into the Android kernel, replacing the conventional unlocking mechanisms. As the user plays the game, biometric features from their touch operations will be recorded and analyzed. The user will only gain access to to the mobile device if the features indicate that they are the intended user (Fig. E)

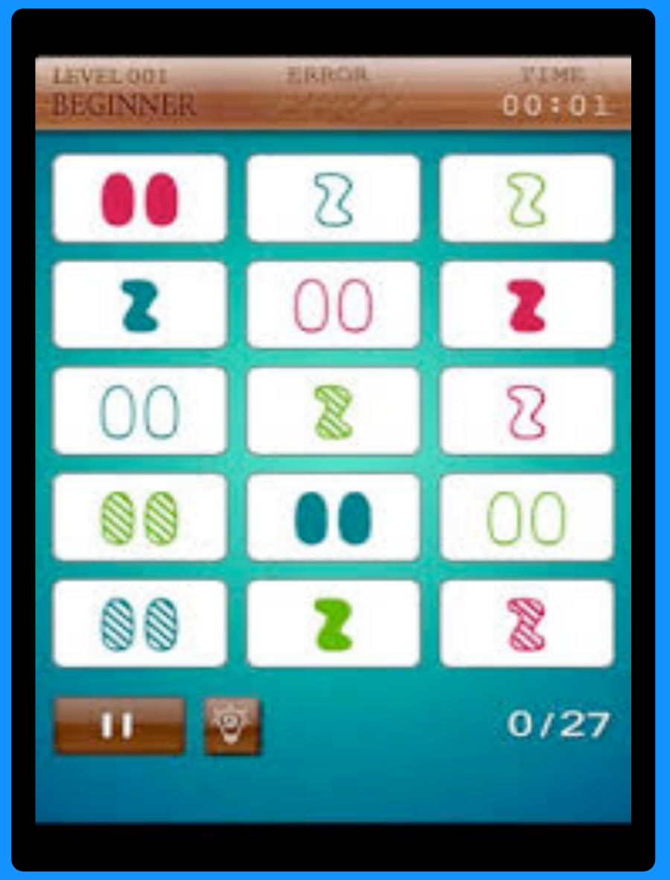
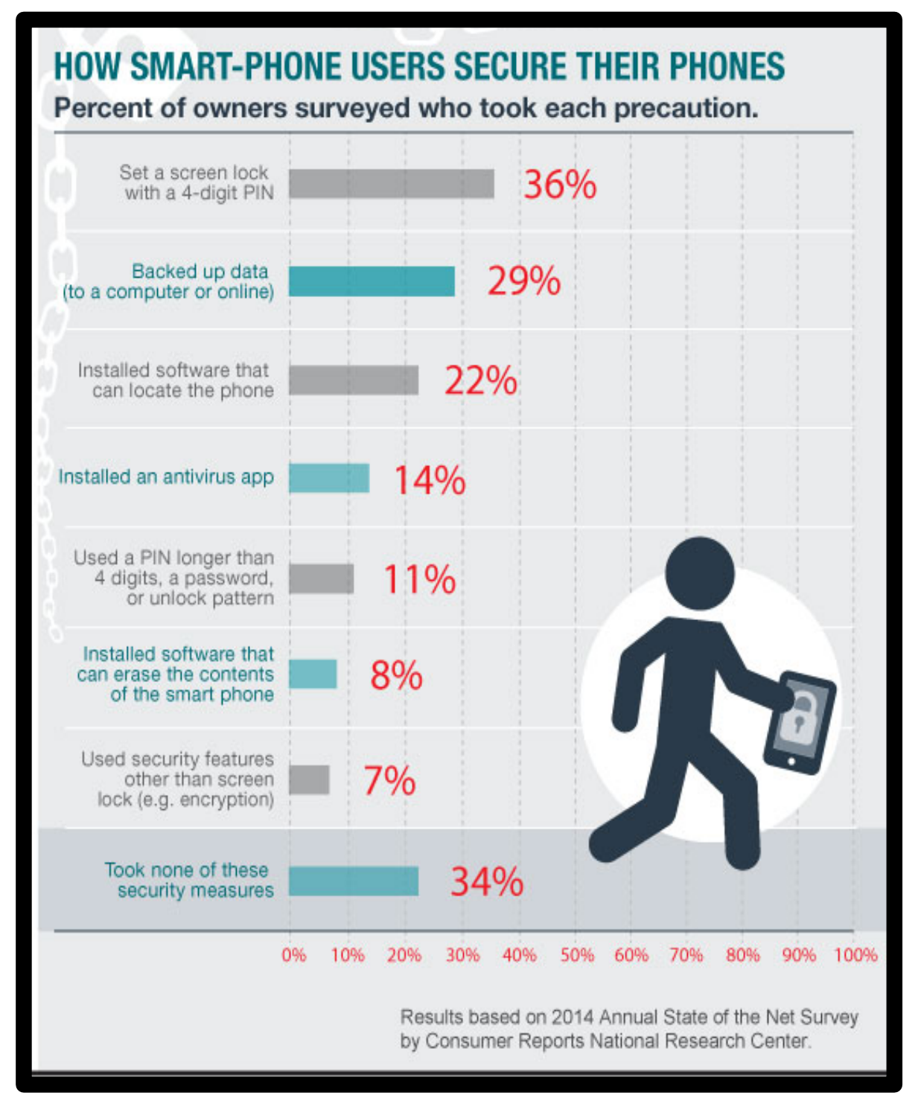


Figure E. A short and simple game will be used to unlock the phone. For example, the game could involve matching, such as SET

Discussion

- **34% of users don't use any locking mechanism on their phones**
- **Biometric user authentication framed in a game eliminates:**
  - Memorizing a passcode
  - Shoulder surfing or smudge attacks
- **Game framing adds entertainment, an incentive to lock phones**



HOW SMART-PHONE USERS SECURE THEIR PHONES

Percent of owners surveyed who took each precaution.

Results based on 2014 Annual State of the Net Survey by Consumer Reports National Research Center.

Future Work

- Create a new game if data analysis indicates that the biometric features are reliable in identification
- Edit the android kernel and insert the new game into it, replacing the original unlocking mechanism.

Android
Software Environment
Applications (built-in & custom)
Application Framework
Libraries & Dalvik Virtual Machine
Linux Kernel

Acknowledgements

The project is funded by the National Science Foundation REU program at the New York Institute of Technology, grant CNS-1263283.

References:

1. Shi, E., Niu, Y., Jakobsson, M., & Chow, R. (2011). Implicit authentication through learning user behavior. In *Information security* (pp. 99-113). Springer Berlin Heidelberg.
2. Xu, H., Zhou, Y., & Lyu, M. R. (2014, July). Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones. In *Symposium On Usable Privacy and Security, SOUPS* (Vol. 14, pp. 187-198).
3. Sitova, Z., Sedenka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., & Balagani, K. (2015). HMOG: A New Biometric Modality for Continuous Authentication of Smartphone Users. *arXiv preprint arXiv:1501.01199*.
4. De Luca, A., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012, May). Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 987-996). ACM.
5. Angulo, J., & Wästlund, E. (2012). Exploring touch-screen biometrics for user identification on smart phones. In *Privacy and Identity Management for Life* (pp. 130-143). Springer Berlin Heidelberg.
6. Bo, C., Zhang, L., Li, X. Y., Huang, Q., & Wang, Y. (2013, September). Silentsense: silent user identification via touch and movement behavioral biometrics. In *Proceedings of the 19th annual international conference on Mobile computing & networking* (pp. 187-190). ACM.
7. Kaminsky, R., Enev, M., & Andersen, E. (2008). Identifying game players with mouse biometrics. *University of Washington, Tech. Rep*.
8. Tapellini, D. (2014, May 1). Smart phone thefts rose to 3.1 million in 2013. Retrieved June 30, 2015.