Smartphone User Trace Analytics

Anand Nirnajan, Swaminathan - University of North Carolina, Charlotte

UNC CHARLOTTE

Analytics~Drives~Innovation
TERADATA. University Network
ANALYTICS CHALLENGE

Our Objective

We intend to achieve security in smartphones beyond single entry authentication by understanding user interaction with the smartphones.

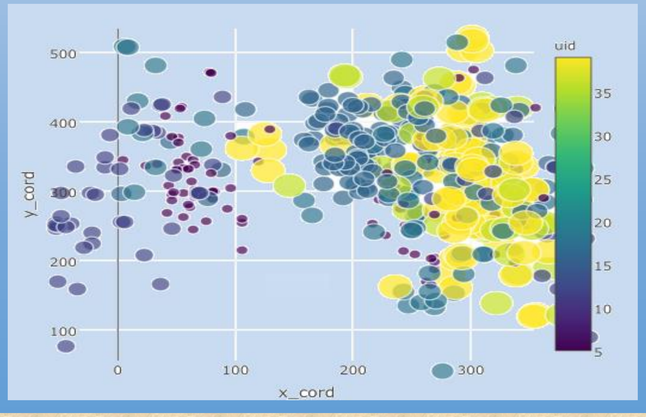
Main Idea

➢Touch patterns of a particular user varies significantly

➢User behavior varies from device to device for the same user.

➢The policies are formulated based on the usage of apps like Wikipedia article, image comparison game and answer questionnaire.

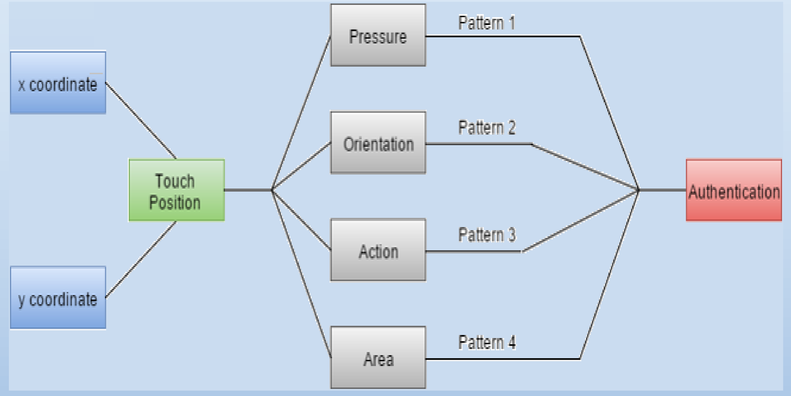
DOT TRACES OF DIFFERENT USERS



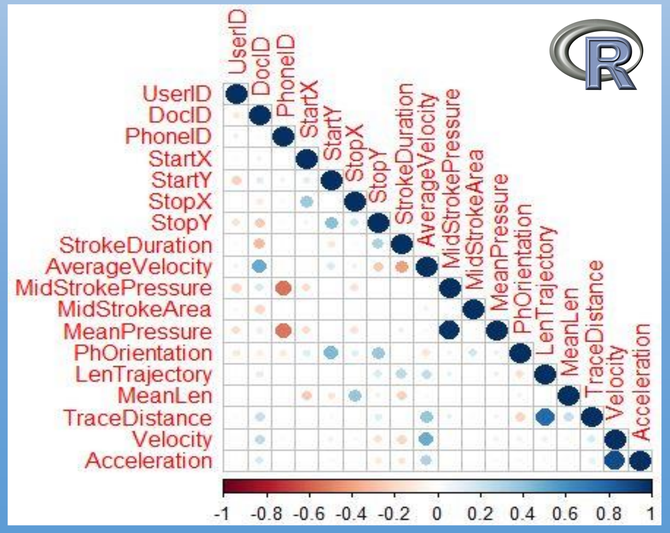
References:

➢Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic and Dawn Song, *"Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication"*, UC Berkeley, Berkeley, December 2012.
➢http://www.mariofrank.net/paper/touchalytics.pdf
➢Dataset - http://www.mariofrank.net/touchalytics/

ANALYSIS STRATEGY



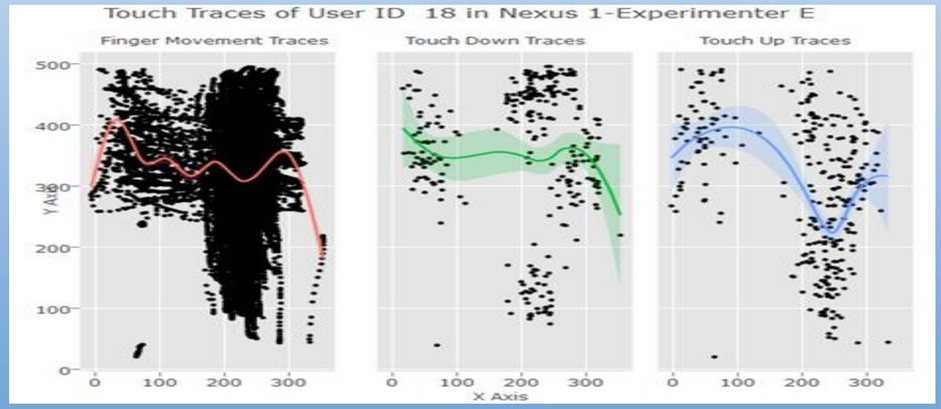
CORRELATION MATRIX



Facts & Findings

➢Stats shows mobile usage increases every year when compared to other devices.
➢As storage of sensitive data increases; breach & threat also increases.
➢ "Average iPhone user unlocks device 80 times per day", says Apple.
➢ 89% of total unlocks comes from Touch ID, this shows the reliability of the security system.
➢Apple has spent 32% more in R&D in 2013 (iPhone 5s released) compared to its previous year.

TOUCH TRACES OF AN USER



Conclusion

➢Smartphone security can be achieved by continuously validating the touch traces of user's touch traces.
➢Extracting more features is essential to improve the accuracy of authenticity so that the access of smartphone by unauthorized uses can be forbidden.