User Authentication Mechanisms on Android

Anshita Agrawal

Advisor
Prof. D.B. Phatak

IIT Bombay, Mumbai
November 3, 2012
## Table of contents

1. **Introduction**
   - Authentication

2. **Entry Point Based Methods**
   - Unlock Patterns
   - Gesture Based Passwords

3. **Continuous or Implicit Authentication**
   - KeyStroke and Mouse Dynamics
   - Pattern Extraction from Users’ Reaction
   - Combination of Behavioural Biometrics over Touchpad
   - Orientation Sensor

4. **Problem Formulation**
   - Motivation

5. **Conclusion and Future Work**
   - Conclusion and Future Work
What is authentication?

- Authentication is the process of determining whether someone or something is, in fact, who or what it claim to be.
- The ways in which someone may be authenticated fall into three categories:
  - something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question)).
  - something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone).
  - something the user is (e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier).
General Authentication Mechanisms

- Passwords
  - Text Based
  - Non Text Based
- Certificates
- Smart Cards
- Biometrics
  - Physiological
  - Behavioural
- Hardware Tokens
- Proximity
Biometric Authentication

- Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits.
- Biometric identifiers are often categorized as physiological versus behavioural characteristics.
- A biometric system operates in the following two modes:
  - Verification Mode
  - Identification Mode
- Performance of a biometric system is measured in terms of the following:
  - False Acceptance Rate
  - False Rejection Rate
  - Equal Error Rate
How it works

Figure: Basic Block Diagram of Biometric System
Challenges

- Recognition performance: How to effectively represent and recognize biometric patterns (e.g., how to recognize a person with 99.999% accuracy)
- System security: How to guarantee that the biometric systems are not vulnerable to sabotage (e.g., can we ensure that fraudsters cannot infiltrate the system?)
- Privacy issues: How to make sure that the biometric system is being exclusively used for the expressed purpose (e.g., how to prevent trusted system administrators from abusing the system)
Unlock Patterns

**Android Screen Unlock Systems**

- Most methods for authenticating users on desktop computers or mobile devices define an entry point into the system.
- The user faces a password challenge and is granted access only if she inputs the correct password.

**Example**

- Slide Lock
- Glass Lock
- Keypad Lock
- Pattern Lock

- These entry-point based methods dominate the authentication schemes today, but they have flaws from both, usability and security perspectives.
Unlock Patterns

Android Screen Unlock Systems

- With this approach an Equal Error Rate of 10.39% has been achieved.
- Two main features captured are: the finger-in-dot time (in milliseconds) and the finger-in-between-dots time.
Gesture Based Passwords

- Existing authentication methods (e.g., alphanumeric passwords) are difficult to remember, especially for individuals with cognitive disabilities that affect memory.
- Here users draw an image using the mouse as their password.
- By associating the password to an object or a concept, the users can easily remember the password.
- Because each user has a unique way in drawing the image, the password is much more secure than simple alphanumeric passwords.
- In addition to the image drawn, it also examine additional measures such as password length, size, angles, and speed to authenticate the user.
Gesture Based Passwords

With this approach an accuracy of 83.3% has been achieved.

The behavioural features exploited are password length, size (the area of the bounding box around the password image), movement speed, start angle and end angle (The start and end angle are the angles formed between the initial and ending line of a gesture respectively with the horizontal line.)
KeyStroke Dynamics

- Keystroke dynamics can be captured via several different features extracted from the typing rhythm of the user.

![Keystroke Metrics](image)

**Figure:** Keystroke Metrics [8]

- It includes latency between consecutive keystrokes, flight time, dwell time, based on the key down/press/up events (as shown in Figure 4), overall typing speed, frequency of errors (use of backspace) and control keys (use of left/right shift).
KeyStroke and Mouse Dynamics

KeyStroke Dynamics

- The latencies, intervals and flight time are measured for each sequence of keystrokes.
- Verification methods are dedicated to verify users based on fixed (static) or variable (free) text inputs. Latter methods can be used in order to verify users continuously.
- Some other metrics that were proposed are:
  - key press duration
  - relative key event order
  - relative keystroke speed
  - classes of shift key usage
  - overlapping of key presses
KeyStroke and Mouse Dynamics

Mouse Dynamics

- Exploiting mouse dynamics for user authentication is less frequently used.
- The study in [8] defines four different mouse actions
  - mouse movement
  - drag and drop
  - point
  - click and silence
- Several different features were defined, such as the interpolation between the movement speed and the traveled distance, which estimates the average speed a user will travel for a certain distance.
KeyStroke and Mouse Dynamics

Mouse Dynamics

- Several histograms were used to capture different working statistics of the user such as the average traveling speed in eight direction zones or the relative occurrence of each one action.

- Features such as the angle, curvature, horizontal, vertical and combined velocity, acceleration and jerk obtained from a vector of data points that were intercepted between two mouse clicks can also be used.

- The accuracy of these methods depends upon the number and type of features used for authentication. And also, the classifier used.
Pattern Extraction from Users’ Reaction

Proposed Methodology

Figure: 3D Graphical Maze
Proposed Methodology

- The user has to steer through the maze for a specified period of time visiting any corridor the user prefers starting from a fixed point.
- The user interaction can be extracted in the form of keystrokes or the turn behaviour of the user.
- Turn behaviour refers to decision of the user at the junctions of vertical and horizontal corridors.
- The decision could be a right turn, left turn, continue in the forward direction (front turn) or turn back and continue in the opposite direction (back turn).
Introduction

Entry Point Based Methods

Continuous or Implicit Authentication

Problem Formulation

Conclusion and Future Work

Pattern Extraction from Users’ Reaction

Behavioral Variables

- For each user, the number of right, left, front, and back turns is calculated.
- These four variables are the first level variables.
- At the second level consecutive pairs of turn directions are considered which results in 16 variables.
- At the third level three consecutive turn directions are considered for a total of 64.
- These three levels of calculations provide the analyser with 84 behavioural variables that can be used in the authentication process.
- The results show an average True Rejection Rate of 88.33% with an average False Acceptance Rate of 11.67%.

Anshita Agrawal

Advisor Prof. D.B.Phatak

User Authentication Mechanisms on Android
Memorable Fingerprint

- This approach is an attempt for generating memorable fingerprint of cellphone users based on their usage patterns.
- It runs on the users cellphone that monitors and records raw events, e.g., SMSes, calls, location, etc.
- The collected raw data is processed and memorable fingerprints are generated.
- The memorable fingerprints generated from rich multi-context data are evaluated by asking each user to answer various authentication questions generated from the fingerprints.
Memorable Fingerprint

![Figure: Memorable Fingerprint](image)

- Results show that the fingerprints generated are remembered by the user to some extent and were moderately secure against attacks even by family members and close friends.
- Accuracy of 84.7% has been achieved.
Combination of Behavioural Biometrics over Touchpad

**Behavioural Variables**

- The behavior information on the pad that can be detected consists of keystroke dynamics and the finger pressure.
- Three features extracted from these behaviors.
- Two features were extracted during the keystroke dynamics: the inter-key and the hold-time.
- Another one feature is the finger pressure which is the force applied over the finger position.
Behavioural Variables

- The results have shown that using only the finger pressure with the k-NN analytical method can indicate users with accuracy rate as 99%.
- The combination of the hold-time and the finger pressure also provided 99% accuracy.
- The interaction of all three metrics i.e. finger pressure, inter-key time and hold time provided an accuracy of 90%.
The orientation sensor is used to obtain the orientation of a smartphone with respect to three axes, namely, x-, y-, and z-axis as depicted in Fig. 7.

**Figure:** Three axes of an orientation sensor [7]
Orientation Sensor

Authentication Based on Orientation of Mobile Device

- Using x-, y- and z-axis a set of 53 orientation-based-biometric features have been defined.
- These features include average, maximum, minimum, range and standard deviation of the angle, angle velocity and angle acceleration.
- k-NN classifier is used for classification.
- This model provided an accuracy of 72%.
Why continuous authentication

- Continuous or implicit authentication approaches would provide an additional line of defense, designed as a non-intrusive and passive security countermeasure.

- These approaches monitor the users interaction with the device, and ideally, at every point in time (or at least with a high frequency) the system estimates if the legitimate user is using the device.

- Hence, a continuous authentication method can either complement entry-point based authentication methods by monitoring the user after a successful login, or, if the method satisfies particular accuracy requirements, it could even substitute entry-point based authentication.
Motivation

Why tablets

- The growing popularity of mobile devices and tablets increases the value of research on their security mechanisms.
- Specifically there are not many existing methods for continuous authentication based on touch biometrics (i.e., without requiring a dedicated activity of the user) and hardly any exploring touch biometrics of a tablet.
- One reason might be the difficulty of extracting a set of sufficiently discriminative features from touch data, because users atomic navigation behavior mostly consists of simple and short movements.
Motivation

Why tablets

- It has been investigated that it is possible to authenticate users while they perform basic navigation steps on a touchscreen device and without any dedicated and explicit security action that requires attention from the user.

- The classifiers achieve robust authentication results, with equal error rates between 0% and 4%, depending on the application scenario.

- The goal here is to analyze how robustly such schemes operate and if they are sufficiently reliable to be used on tablets.

- There are differences between smart phones and tablet computers that might make it harder to continuously authenticate users on tablets.
Why tablets

- The small size of the screen of smartphones helps continuous authentication.
- The reason is that content of documents, emails, image collections, menus, or icon collections hardly fit on the smartphone screen in most application scenarios.
- As a result, the user must move around screen content and thus the classifier gets a lot of observations over time.
- In contrast, on large tablet screens users can read for a long time without scrolling, all icons fit on screen, and so on.
- This might reduce the strokes per minute below a rate that can be considered secure.
- Moreover, the large screen introduces more degrees of freedom.
Motivation

Proposed Approach

- A continuous authentication application could run in the background and extract multiple features from all available raw input.
- This raw input is readily available through the phones API.
- Based on various extracted features, the system can then learn a profile of the legitimate user and compare all screen interaction with this profile.
- There are two phases for learning and classifying touch behavior.
  - Enrollment Phase
  - Continuous Authentication Phase
Proposed Approach

- During the enrollment phase, the system monitors the touch biometrics and extracts particular features from the touch data.
- This process continues until the distribution of touch-features converges to an equilibrium.
- This is the point in time when one can assume that:
  - the user got used to her device and her device-specific touch-skills no longer improve.
  - the system has observed sufficiently many strokes to have a stable estimate of the true underlying feature distribution of that user.
- At that point, the system can train the classifiers and switch to the classification mode for authentication.
Proposed Approach

- Once the classifiers are trained, the device begins the authentication phase.
- During this phase, the system continuously tracks all strokes and the classifier estimates if they were made by the legitimate user.
- For $t$ consecutive negative classification results, the system resorts back to the initial entry-point based authentication method and challenges the user.
- The precision of the individual classifiers influences the choice of $t$. 
Classification Method

- The first step of feature-extraction is to divide up the data records into individual strokes.
- A stroke is a sequence of touch data that begins with touching the screen and ends with lifting the finger.
- Android API can log the 8 raw features which includes time[ms], action(touch up, touch down, move), phone orientation, x-coordinate, y-coordinate, pressure, area covered, finger orientation.
- A set of 30 behavioral touch features of a stroke can then be extracted from raw data which are shown.
**Classification Features**

- inter-stroke time, stroke duration
- start x, start y, stop x, stop y
- direct end-to-end distance
- mean resultant length
- up/down/left/right flag
- direction of end-to-end line
- pairwise velocity
- median velocity at last 3 pts
- largest deviation from end-to-end line
- average direction
- average velocity
- mid-stroke pressure
- mid-stroke area covered
Motivation

Classification Method

- Different users populate distinct subspaces of this feature space.
- The feature set is then fed to k-NN classifier for making the authentication decision.
- The kNN classifier takes every new observation (here: a stroke) and locates it in feature space with respect to all training observations.
- The classifier identifies the k training observations that are closest to the new observation.
- Then, it selects the label that the majority of the k closest training observations have.
Conclusion

- Authentication mechanisms for user authentication based on single entry point and continuous authentication have been studied.
- Implicit or continuous authentication method can either complement entry-point based authentication methods by monitoring the user after a successful login, or, if the method satisfies particular accuracy requirements, it could even substitute entry-point based authentication.
- A classification framework has been analyzed for classifying the feature set extracted from the user interaction with the touchscreen of the mobile device to investigate if it is possible to authenticate users while they perform basic navigation steps on a touchscreen device.
Future Work

- Analysis and investigation of how robustly implicit authentication schemes will operate on tablet will be done.
- If they are sufficiently reliable to be used on tablets will be tested.
- An application to test the feasibility and accuracy of the proposed approach will be devised.
- Feature set for improving the efficiency and accuracy of the classification framework will be explored.
Ahmed Al-Khazzar and Nick Savage.  
Graphical authentication based on user behaviour.  

Julio Angulo and Erik Wstlund.  
Exploring touch-screen biometrics for user identification on smart phones.  

M. Belkhede, V. Gulhane, and P. Bajaj.
Biometric mechanism for enhanced security of online transaction on android system: A design approach.


V. Conti, S. Vitabile, and F. Sorbello.
Fingerprint traits and rsa algorithm fusion technique.

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.
Human: Creating memorable fingerprints of mobile users.
In *PerCom Workshops’12*, pages 479–482, 2012.

Chien-Cheng Lin, Deron Liang, Chin-Chun Chang, and Ching-Han Yang.
A new non-intrusive authentication method based on the orientation sensor for smartphone users.

Robert Moskovitch, Clint Feher, Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet Camtepe, Bernhard Löhlein, Ulrich Heister, Sebastian Möller, Lior Rokach, and Yuval Elovici.
Introduction

Entry Point Based Methods

Continuous or Implicit Authentication

Problem Formulation

Conclusion and Future Work

Identity theft, computers and behavioral biometrics.


R. Mukesh and V.J. Subashini.
Fingerprint based authentication system using threshold visual cryptographic technique.
In Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on, pages 16 –19, march 2012.

H. Saevanee and P. Bhatarakosol.
User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device.
Conclusion and Future Work


**Kwang Il Shin, Ji Soo Park, Jae Yong Lee, and Jong Hyuk Park.**

Design and implementation of improved authentication system for android smartphone users.


**L. Sreeramareddy, J. Feng, and A. Sears.**

Poster: Preliminary investigation of gesture-based password: Integrating additional user behavioral features.