

UNIVERSITY OF TARTU  
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE  
Institute of Computer Science

ENNO ELLER

# Simplifying Mobile Social Media Authentication On Android

Bachelor Thesis (6 EAP)

*Supervisor: Huber Raul Flores Macario, M.Sc*  
*Co-supervisor: Satish Narayana Srirama, Ph.D*

**Author:..... "....." May 2015**

**Supervisor:..... "....." May 2015**

**Professor:..... "....." May 2015**

TARTU, 2015

## **Abstract**

Smartphones are very common nowadays and people all around the world are using them in their everyday life. Even though mobile phones were originally invented as calling devices, smartphones allow the user to communicate in different ways including social media, which as of January 2014, 74% of online adults use. In case they own a smartphone, they probably use social media on it as well, but with restrictions that come with the size of the device, affecting how we view content and also type. Typing on smartphones can be frustrating, but more so when the keyboard size prevents us from succeeding with authentication and we have to type the same text numerous times. This paper proposes a solution to such occurrences by using pattern recognition rather than typing. Patterns allow the screen to be used more efficiently, giving the user more room for accuracy errors. Survey results indicate that approaching authentication in this way is feasible.

# Contents

<b>List of Figures</b>	<b>v</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.1.1 Motivation . . . . .	1
1.1.2 Contributions . . . . .	1
1.1.3 Outline . . . . .	1
<b>2 State of the Art</b>	<b>3</b>
2.1 Authentication Process Usability . . . . .	3
2.1.1 Android AccountManager . . . . .	3
2.1.2 Service providers . . . . .	3
2.1.2.1 Google Identity Platform . . . . .	4
2.1.2.2 Facebook SDK . . . . .	4
2.2 Previous work . . . . .	4
2.2.1 Visual login . . . . .	4
2.2.2 Tap pattern . . . . .	4
2.2.3 Fingerphoto recognition . . . . .	5
2.2.4 Token-based authentication . . . . .	5
2.2.5 Arms flex . . . . .	5
2.2.6 Multitouch image-based authentication . . . . .	5
2.2.7 Continous authentication . . . . .	6
2.2.7.1 Gait recognition . . . . .	6
2.2.7.2 Keystroke analysis . . . . .	6
2.2.7.3 Location information . . . . .	6

## CONTENTS

---

2.2.7.4	Orientation sensor . . . . .	7
2.2.7.5	TouchScreen gestures . . . . .	7
2.3	Summary . . . . .	7
<b>3</b>	<b>Problem Statement</b>	<b>9</b>
3.1	Research Question . . . . .	9
3.2	Summary . . . . .	9
<b>4</b>	<b>Your Contribution</b>	<b>11</b>
4.1	Your Brilliant Ideas ... . . . .	11
4.2	Summary . . . . .	11
<b>5</b>	<b>Case Studies</b>	<b>13</b>
5.1	Case of Study... . . . .	13
5.2	Summary . . . . .	13
<b>6</b>	<b>Conclusions</b>	<b>15</b>
<b>7</b>	<b>Related Work</b>	<b>17</b>
<b>8</b>	<b>Future Research Directions</b>	<b>19</b>
<b>9</b>	<b>Sisukokkuvõte</b>	<b>21</b>
	<b>Bibliography</b>	<b>23</b>

# List of Figures

## LIST OF FIGURES

---

# 1

## Introduction

### 1.1 Introduction

Briefly summarize the question (you will be stating the question in detail later), and perhaps give an overview of your main results. (it is not just a description of the contents of each section)

#### 1.1.1 Motivation

Some of the reasons why it is a worthwhile question.

#### 1.1.2 Contributions

Solution developed - (e.g. algorithm, tools, etc.)

#### 1.1.3 Outline

Brief introduction of each chapter

## 1. INTRODUCTION

---



## 2

# State of the Art

### 2.1 Authentication Process Usability

Authentication process usability in this context refers to automating or simplifying the process of authenticating the user accessing the phone or features on the phone. This section discusses some of the tools used on mobile phones or tablets to simplify authentication.

#### 2.1.1 Android AccountManager

Most of the applications are using Android AccountManager as a tool to automate authentication. It is a built in centralized registry that can hold user credentials or even authentication tokens which are generated via application server. Though it requires implementing various components, increasing the complexity, it is still a good method for single user device. For example Google, Facebook, and Microsoft Exchange each use this method. (1)

#### 2.1.2 Service providers

The next most used method of authentication is provided by social media websites. These providers are giving developers the option to let users authenticate by using accounts on the social media websites. Users do not have to create new accounts to these sites, but will refer to their already existing accounts on social media as a way of registration. On android the user needs to have that social media application installed

## 2. STATE OF THE ART

---

and logged in to use this method. The most known two providers are Google and Facebook.

### 2.1.2.1 Google Identity Platform

Google is providing android developers with an application programming interface (API) which allows users to register and authenticate using Google account, but also allows developers to integrate other Google services into their applications: payments via Google Wallet, sharing with Google+, saving files to Drive, etc. (2)

### 2.1.2.2 Facebook SDK

Facebook has a software development kit (SDK) for android developers. Just as with Google API, the SDK allows authentication via Facebook account and also provides more services - sharing on Facebook, sending application invites via Facebook, etc. (3)

## 2.2 Previous work

### 2.2.1 Visual login

Visual login refers to a class of mechanisms that rely on the selection of icons or photo images to produce a password value. Visual login is a knowledge-based approach like passwords. Instead of alphanumeric characters, users must remember image sequences. Visual images are presented to the user for selection by tiling a portion of the users graphical interface window with identically sized squares, grouped into a 5 x 6 matrix. The surface of each square displays a bit-mapped image or thumbnail of some picture supplied in a predefined digital format. Selecting the correct sequence of thumbnail images authenticates the user to the device. (4)

### 2.2.2 Tap pattern

Gesture interaction with mobile devices has become common-place. One class of gestures that is widely used is tapping. While key strokes are usually perceived as single events, taps have an implied duration in time. Single taps, long presses and double taps are common examples. These simple patterns can be detected efficiently with very crude algorithms, relying solely on timers. Tap patterns, however, can be more

generally defined as a sequence of intervals of on and off times that is, the ordered time distances between and within taps. (5)

### 2.2.3 Fingerphoto recognition

The intention of the fingerphoto recognition is that for authentication the user simply positions his finger close in front of the camera in order to capture a biometric sample. The algorithms for finger detection and quality assurance check continuously the pre-view images of the camera after the capture process has been initiated by the user. The results of the algorithms are calculated in real-time and are displayed on the graphical user interface. A photo is automatically taken when all criteria for the fingerphoto recognition are fulfilled. (6)

### 2.2.4 Token-based authentication

Authentication on smartphones does not have to include doing something to or with the device, instead it can involve a physical token. The token can be so small it could be carried on a key chain and it automatically unlocks the smartphone whenever its owner wants to use it. The token is based on magnetic fields detected by the smartphones compass or on an acoustic transmitter that generates a signal picked up by the handsets microphone. All the user has to do is carry the token with him. (7)

### 2.2.5 Arms flex

One of the human behaviors considered being unique is arms flex. It is gestural pattern i.e. the way people bend their arm for picking a phone when responding to incoming calls. That arms flexing is considered as a subset of gesture pattern in lower limb gesture. Every person who bends their arm will have different strength measured by accelerometer using smartphone even if they own same arms flex pattern visually.(8)

### 2.2.6 Multitouch image-based authentication

Multitouch image-based authentication password can consist of multiple rounds, where in each round the user can mark multiple points on an image. Click points have the advantage that they can be entered quickly, even with multiple fingers simultaneously, while drawing complex patterns requires more time. Multitouch authentication uses

## 2. STATE OF THE ART

---

background images as cues and determines the image for the next round based on the users input in the current round. Thus, the user can instantly recognize if the points selected in the previous round were correct or wrong (expected vs. unexpected image in next round). A back button allows for correction of errors. Each image should also only appear once in a password sequence to prevent memory interference between two instances of the same image. (9)

### 2.2.7 Continous authentication

It is not always good to have a phone authenticate the user once and let him keep using the phone till it gets locked automatically by a timer or physically by the user. Hence there are methods that monitor the phone even when the phone is unlocked and only when there is sufficient evidence that the current user is not the smartphone owner, traditional user authentication is activated.

#### 2.2.7.1 Gait recognition

The term gait recognition describes a biometric method which allows an automatic verification of the identity of a person by the way he walks. Gait recognition is based on wearing motion recording sensors on the body in different places: on the waist, in pockets. The wearable sensors can be accelerometers (measuring acceleration), gyro sensors (measuring rotation and number of degrees per second of rotation), force sensors (measuring the force when walking) etc. (10)

#### 2.2.7.2 Keystroke analysis

This method of authentication analysis the detailed timing information that describes exactly when each key was pressed and when it was released by the person typing. (11)

#### 2.2.7.3 Location information

Phones and tablets nowadays come with built-in GPS systems. GPS individually or in cooperation with cell towers allows a phone to acquire its current location which is analysed against previous data. (12)

### 2.2.7.4 Orientation sensor

A user has a unique way to hold and operate his/her smartphone while working on some applications and such behavioral biometrics can be captured from the readings of the orientation sensor. Users behavioral biometrics of up-down flicks and left-right flicks from the orientation sensor are monitored to authenticate. (13)

### 2.2.7.5 TouchScreen gestures

As long as the smartphone is used, gestures are monitored to authenticate the user continuously. Continuous authentication is done on the background using intercepted touch data from normal user-smartphone interactions. The detection approach is invoked on-demand whenever touch inputs are received and is transparent to the smartphone user. Selected touch gesture information are collected including gesture type, X and Y coordinates, directions of the finger motion, finger motion speed, pressure at each sampled touch point and the distance between multi-touch points. In total, there are 53 features for each touch gesture. The six most frequent and useful gestures: down to up swipe, up to down swipe, left to right swipe, right to left swipe, zoom-in, and zoom-out. Since a smartphone user may apply different levels of touch pressure at different stages of a touch gesture, they are divided into three segments, (i) the beginning of a touch motion, (ii) the main touch motion, which is the longest segment and (iii) the end of a touch motion. (14, 15)

## 2.3 Summary

Using 3rd party accounts as means for authentication is viable in many situations, but it also requires accounts on these sites, which makes the application bound to theirs. Writing your own code for simplifying authentication does not bound the application to anyone, at the same time could mean more work on the coding.

## 2. STATE OF THE ART

---

## 3

# Problem Statement

Transition - Since the establishment of SyncML by the Open Handset Alliance (OHA); the synchronization of data is the adopted approach for supplying cloud resources to the handset...

### 3.1 Research Question

Engineering theses tend to refer to a problem to be solved where other disciplines talk in terms of a question to be answered. In either case, this section has three main parts: 1. a concise statement of the question that your thesis tackles 2. justification, by direct reference to section 3, that your question is previously unanswered 3. discussion of why it is worthwhile to answer this question.

### 3.2 Summary

To counter the problems with the interoperability across multiple clouds, to perform data-intensive processing invocation from the handset and to introduce the platform independence feature for the mobile cloud applications, the following thesis discusses a Mobile Cloud Middleware (MCM) (? ). The middleware provides a unique interface for mobile connection and multiple internal interfaces and adapters, which manage the connection and communication between different clouds. The MCM capabilities for managing the resource intensive tasks can easily be envisioned in several scenarios which are discussed in further sections as case of study.

### 3. PROBLEM STATEMENT

---



## 4

# Your Contribution

Transition - Several are the issues that were discussed in previous chapter, regarding the use of cloud services from the mobile...

### 4.1 Your Brilliant Ideas ...

This part of the thesis is much more free-form. It may have one or several sections and subsections. But it all has only one purpose: to convince the examiners that you answered the question or solved the problem that you set for yourself in Section 4. Here, you have to present. Your brilliant idea(s), description, mathematical model that support your idea(s), analysis of the solution (e.g. performance, scalability, etc.)

### 4.2 Summary

Summarize the chapter with at least two paragraphs.

#### 4. YOUR CONTRIBUTION

---

# 5

## Case Studies

Transition - The development of mobile applications that requires data-intensive processing and at the same time that keeps a tolerable interaction with the user, its feasible though the use...

### 5.1 Case of Study...

### 5.2 Summary

Summarize the chapter with at least two paragraphs.

## 5. CASE STUDIES

---

## 6

# Conclusions

Summarize your work and results.

## 6. CONCLUSIONS

---

## 7

# Related Work

Compare your solution with existing projects. How your solution is better than the others?, why to use your solution?, etc.

## 7. RELATED WORK

---



8

## Future Research Directions

Briefly indicate how your current research can be extended, some improvements, etc.

## 8. FUTURE RESEARCH DIRECTIONS

---

9

## Sisukokkuvõte

Eesti abstract...

## 9. SISUKOKKUVÕTE

---

# Bibliography

- [1] Android accountmanager.  
URL <http://developer.android.com/reference/android/accounts/AccountManager.html>
- [2] Google identity platform.  
URL <https://developers.google.com/identity/>
- [3] Facebook sdk.  
URL <https://developers.facebook.com/docs/android>
- [4] W. Jansen, Authenticating users on handheld devices, in: Proceedings of the Canadian Information Technology Security Symposium, 2003, pp. 4–6. 4
- [5] D. Marques, T. Guerreiro, L. Duarte, L. Carriço, Under the table: Tap authentication for smartphones, in: Proceedings of the 27th International BCS Human Computer Interaction Conference, British Computer Society, 2013, p. 33. 5
- [6] C. Stein, C. Nickel, C. Busch, Fingerphoto recognition with smartphone cameras, in: Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the, IEEE, 2012, pp. 1–12. 5
- [7] H. Bojinov, D. Boneh, Mobile token-based authentication on a budget, in: Proceedings of the 12th Workshop on Mobile Computing Systems and Applications, ACM, 2011, pp. 14–19. 5
- [8] A. F. P. Negara, E. Kodirov, M. F. A. Abdullah, D.-J. Choi, G.-S. Lee, S. Sayeed, Arms flex when responding call for implicit user authentication in smartphone, *Int. J. Secur. Its Appl* 6 (2012) 879–83. 5
- [9] D. Ritter, F. Schaub, M. Walch, M. Weber, Miba: Multitouch image-based authentication on smartphones, in: CHI'13 Extended Abstracts on Human Factors in Computing Systems, ACM, 2013, pp. 787–792. 6
- [10] M. O. Derawi, C. Nickel, P. Bours, C. Busch, Unobtrusive user-authentication on mobile phones using biometric gait recognition, in: Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on, IEEE, 2010, pp. 306–311. 6
- [11] A. Buchoux, N. L. Clarke, Deployment of keystroke analysis on a smartphone, in: Australian Information Security Management Conference, 2008, p. 48. 6
- [12] H. Takamizawa, N. Tanaka, Authentication system using location information on ipad or smartphone, *International Journal of Computer Theory and Engineering* 4 (2) (2012) 153–157. 6
- [13] C.-C. Lin, D. Liang, C.-C. Chang, C.-H. Yang, A new non-intrusive authentication method based on the orientation sensor for smartphone users, in: Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference on, IEEE, 2012, pp. 245–252. 7
- [14] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, N. Nguyen, Continuous mobile authentication using touchscreen gestures, in: Homeland Security (HST), 2012 IEEE Conference on Technologies for, IEEE, 2012, pp. 451–456. 7
- [15] L. Li, X. Zhao, G. Xue, Unobservable re-authentication for smartphones., in: NDSS, 2013. 7