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

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

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

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 research

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 preview 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

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)

2.3 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.

2.3.1 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)

2.3.2 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)

2.3.3 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)

2.3.4 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)

2.3.5 TouchScreen gestures

As long as the smartphone is used, gestures are monitored to authenticate the user continuously. Continuous authentication in 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)

2.4 Summary

The world of android and mobile in general is filled with means to authenticate the user. All of the methods discussed have their advantages and disadvantages, but they all serve the same purpose of keeping our device and data secure.

3

Problem Statement

In the few years previous to 2010, tablets started to circle the market and nobody saw exactly how it would affect the devices we own. In 2010 Steve Jobs, the co-founder of Apple Incorporation, predicted that tablets would overtake PCs (personal computer). Slowly tablets have reduced the sales gap and in 2015 that prediction will probably come true. (16)

Though PCs will not go anywhere in the near future, it still means that tablets and phones are becoming the main tools for people to access social media. That in mind, when we look at these devices, we can immediately notice the size and lack of peripherals compared to PCs, raising the concern of input difficulty. In particular, inputting complicated passwords, that require precision to the last letter.

Those, with more knowledge and use experience with Android devices will recall that Android devices usually keep applications logged in with no need to re-authenticate. Though that is mainly true, there are cases, where re-authentication is necessary. Android tends to log out the user, when the applicaton is updated.

As mentioned previously, Android devices are becoming common for households and therefore these devices need to accompany not only one, but many users raising the second and more common case for re-authentication.

3.1 Research Question

How to make Android devices more compatible with multiple users by simplifying auhentication?

3.2 Summary

As Android devices are slowly taking over from PCs it needs to pick up some of PCs attributes. The following sections focus on a solution to make Android devices for multiple users. This solution is developed as a part of this thesis.

4

Your Contribution

In Chapter 2 multiple alternatives to automating authentication were discussed. This section will focus on the solution developed as part of this theses.

4.1 Short description of the solution

This solution is not an application being installed on a device, but is a library that developers can apply in their applications with very little coding. All needed to do is import the library into a project and refer to it.

The library provides easy registration for new credentials, storing them and retrieving for authentication. The user only inserts the credentials once and protects them with a pattern which is used for retrieving them. The pattern and the credentials are stored locally in a database, which is application specific and can only be accessed by it.

An exapmle project is used in this paper for demonstation puproses.

4.2 Android lockpattern

As mentioned in the previous section a pattern is used to protect the credentials. Android users might already be familiar with the lockpattern even when they have not heard the term itself. It is used for locking the device from unwanted access to it, shown in the Figure 4.1. It is a 3x3 matrix consisting of circles/dots. To draw a pattern a user must press on a circle and drag through others to make a pattern and release to verify it. Even though the user only sees a picture of the pattern it is actually a string of numbers representing the dots where the user changed direction. For example a string "1-7-8" would be a pattern "L". Android lockpattern is known to users and is very easy to understand. Typing is taken out of the authentication process, which reduces the amount of errors made, and therefore used in this solution.

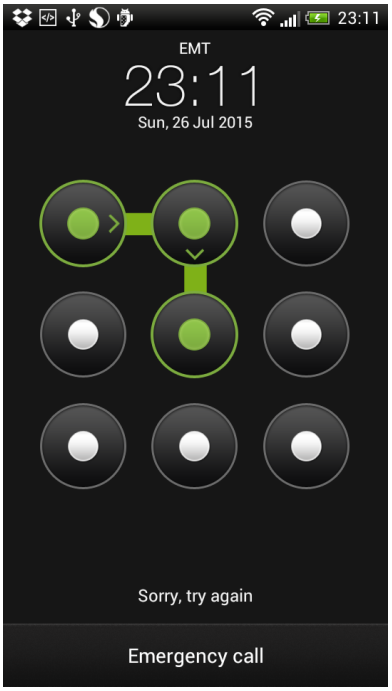

Figure 4.1: Android lockpattern

4.3 Supporting Multiple Users

The key factor what makes it different from previous solutions is the support for multiple users. Credentials for user authentication is kept in a local database accessed only by the application.

4.4 Summary

Summarize the chapter with at least two paragraphs.

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.

6

Conclusions

Summarize your work and results.

7

Related Work

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

8

Future Research Directions

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

8. FUTURE RESEARCH DIRECTIONS

9

Sisukokkuvõte

Eesti abstract...

Bibliography

[1] Android accountmanager.
URL http://developer.android.com/reference/android/accounts/AccountManager.html 3

[2] Google identity platform.
URL https://developers.google.com/identity/ 4

[3] Facebook sdk.
URL https://developers.facebook.com/docs/android 4

[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

[16] [link].
URL http://www.extremetech.com/computing/185937-in-2015-tablet-sales-will-finally-surpass-pcs-fulfilling-steve-jobs-post-pc-prophecy 9