Graphical-Based User Authentication Schemes for Mobile Devices Evaluation

Vitaly Petrov, Alexandra Afanasyeva
SUAI, St. Petersburg, Russia
{vit.petrov, alra}@vu.spb.ru

Abstract

Huge amount of personal information is stored in the mobile devices now. This requires high-qualified security system in order to provide data confidentiality, if the device is lost or stolen. The main part of such system is an authentication module, and there are several methods used to solve this problem. However, traditional schemes, based on usage of text passwords, are not suitable for mobile devices because of their drawbacks. The main drawbacks are bad memorability [1] and inconvenience for the user, if the device does not have a hardware keyboard. In this case Graphical Passwords (GP) can become a good alternative, because of better memorability [1], ease of input on a touchscreen, and even higher security level [2].

But despite the presence of some good enough GP schemes, there is no persuasive method to compare them. While the field investigation, which is expensive, subjective and difficult to repeat, is the only way used to evaluate the usability level, common technique to assess the level of security does not exist at all. And the main goal of the project is to propose novel automated and theoretical methods to evaluate the security level of different GP schemes widely used in mobile devices.

From the security point of view all such systems can be split into two classes: PIN-equivalents and passphrases analogues. Schemes from the first group can be used only during switching on or unlocking the device, while stronger systems may replace traditional authentication methods even in personal data storage. Meanwhile, in [2] and [3] another classification is proposed according to the algorithms used in different schemes. And in this paper only systems of Draw-a-Secret type [4] are considered.

As a quantitative metrics to evaluate the security level, false negative error rate and false positive error rate [5] are proposed. And as an automated method of comparison we suggest using a test bench with three modules.

1) *GUI module* is a basic part and used to evaluate manually the chosen GP scheme in order to form a subjective opinion.
2) *Text module* provides a possibility to automatically compare chosen authentication systems on a specified number of test cases.
3) *User behaviour modeling module* works as a tool to create a set of test cases for the Text module.

The idea of User behaviour modeling is producing test cases from a password, stored in the authentication system. There are two sets of changes: good and bad. First includes turning, scaling, and moving, and makes GP that are valid too. By adding to the true password new intersections and lines, and moving point (bad changes) User behaviour module can create invalid passwords. So the test case is a pair of a password, for which system should choose is it valid or not, and a true answer for this question. If GP scheme approves an invalid password, that is a false negative error; if scheme denies access for a person with a valid password, that is a false positive error. The less the authentication system makes faults, the better it is.

We propose the following algorithm of usage for this test bench.

1) Choose an authentication scheme and train it with a specified password.
2) Use this password and User behaviour model module to produce a set of test cases.
3) If there is a necessity to add some particular test cases manually, draw and save them with a GUI module.
4) Start the Text module and initiate the testing procedure.

5) Finally, get false negative error rate and false positive error rate for the chosen system.

To prove the results got from the test bench some theoretical assessments are suggested. Firstly, by analogy with text passwords, the cardinality of set of all possible passwords should be estimated. Sometimes it is non-trivial or even impossible task. Moreover, it is necessary not only to calculate the cardinality of this set, but also to evaluate the probability distribution. Currently, we are trying to chose a metric for this, considering variance and entropy.

Index Terms: Graphical Password, Security, Authentication.

REFERENCES

[1] A. Paivio, ”Mind and Its Evolution: A Dual Coding Theoretical Approach”, *Lawrence Erlbaum: Mahwah*, N.J., 2006

[2] R. Biddle, S. Chiasson, P.C. van Oorschot, ”Graphical Passwords: Learning from Fisrt Generation”, *Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada*, 2009

[3] R. Weiss and A. De Luca, ”PassShapes - utilizing stroke based authentication to increase password memorability”, *NordiCHI, ACM*, pp. 383-392, 2008

[4] I. Jermyn, A. Mayer, F. Monrose, M. Reiter and A. Rubin, ”The design and analysis of graphical passwords”, *8th USEFIX Security Symposium*, 1999

[5] F. David, ”Probability Theory for Statistical Methods”, *Cambridge University Press*, p. 28, 1949