Session Passwords for Android Mobiles

S. Archana, T. Meena, A. S. Vaishnavi & A. Bazila Banu

Department of Information Technology,
Velammal College of Engineering and Technology, Madurai-625 009, Tamil Nadu, India
E-mail : sarchanamdu@gmail.com, dewdropmt@gmail.com, vaishnavishivanath@gmail.com, abb@vcet.ac.in

***Abstract* – The mobiles that are marketed today are developed with extended features that include the data storage. To protect the data most people make use of the textual passwords or Graphical passwords in spite of its high security issues such as eavesdropping, dictionary attacks, social engineering and shoulder surfing. Hence as a milestone in the field of security, the experts developed the idea of Session password that has come into existence. This paper involves the implementation of two techniques that combine the texts and colors to generate session passwords. One of the techniques involve a 6*6 alphanumeric matrix while the other includes a color palette along with a numeric matrix that are unlocked using the concepts of playfair cipher cryptographic method for the high rate of security in android mobiles.**

Keywords – Authentication, Session passwords, Security

I. INTRODUCTION

Security in mobiles has become a major concern for its users. From Android to Symbian and even, most iOS in the mobile market are targeted by the malicious hackers. At the same time people have also started to know about mobile security and they have began their search for new technologies that safeguard them from the mobile threats. Since a sheer number of people have started using android, it has become a chief target for the malicious hackers. Yet many people do not believe that android security is a major threat to them.

Many authentication techniques have been developed to protect the mobiles from the existing and evolving threats. One of the techniques that are used widely today is the textual password. This practice is subjected to many vulnerabilities like eves dropping, dictionary attack, social engineering, shoulder surfing and even. Though lengthy and random passwords increase the security, the main problem in this method is the difficulty of remembering those passwords. In order to eliminate this intricacy many users tend to pick short passwords or passwords that they could remember easily. The shortcoming of this technique is that these passwords can be easily guessed and cracked. The alternatives to this practice are graphical passwords and biometrics. These methods are also accounted with their own disadvantages. Biometrics that deal with finger prints, iris scan or facial recognition provide more security still they are not used in wide because it is highly expensive and its identification process is slow. Many graphical passwords have been developed in the last decade which suffer shoulder surfing. There are even graphical passwords schemes that resist shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Thus new authentication methods have to be developed to protect mobiles or any PDAs that are used to store confidential information like PIN number or passwords etc.

In this paper we have explained about the implementation procedure of two authentication schemes that increases the mobile security. The authentication here is carried out using session passwords. Session passwords are dynamic passwords that change each and every time the user logs in. That is, once the session is terminated the password is no longer useful. For every login, users input different passwords that provide better security against dictionary and brute force attacks. The proposed authentication schemes use text and colors for generating session passwords.

II. MATERIALS AND METHODS

Android [17] being a Linux based OS is predominantly used for touch screen devices. The user interface is based on direct manipulation, using touch inputs that loosely correspond to real world actions like tapping, swapping and even to manipulate on-screen objects. The drag and drop tools in the resource folder is used in designing the UI. Completing the UI, the logics are written using JAVA.

The SQLite database [18] that has been used is a software library that implements a self-contained, server less, zero-configuration, transactional SQL database engine. The source code for SQLite is in the public domain. Android applications run in a sandbox, an isolated area of the system that does not have access to the rest of the system's resources, unless access permissions are explicitly granted by the user when the application is installed.

III. MOTIVATION AND OBJECTIVE

Security and usability are considered as the most important factors of the system design that increase the user friendliness of the system. Android mobile is one such system that requires high user friendliness. Since the attack on android mobiles has increased in present times, highly secured authentication scheme has become a necessary. Most secured schemes compensate with their usability which becomes a shortcoming on the other hand. Thus the main objective of our paper is to implement an authentication scheme to android mobiles, providing both usability and security by combining colors with numbers and texts.

IV. RELATED WORK

1) RECALL-BASED SYSTEMS

Recall-based graphical password systems are occasionally referred to as *draw metric systems* [1] because users recall and reproduce a secret drawing. In these systems, users typically draw their password either on a blank canvas or on a grid.

DRAW-A-SECRET

Draw-A-Secret (DAS) [2] was the first recall-based graphical password system proposed. Users draw their password on a 2D grid using a stylus or mouse. A drawing can consist of one continuous pen stroke or preferably several strokes separated by "pen-ups" that restart the next stroke in a different cell. To log in, users repeat the same path through the grid cells. The system encodes the user-drawn password as the sequence of coordinates of the grid cells passed through in the drawing, yielding an *encoded* DAS password. Its length is the number of coordinate pairs summing across all strokes.

PASSDOODLE

Pass doodle [3-4] is similar to DAS, allowing users to create a freehand drawing as a password, but uses more complex matching process without a visible grid. The use of additional characteristics such as pen color, number of pen strokes, and drawing speed were suggested to add variability to the doodles.

PASS GO

The Pass-Go scheme designed by [5] was motivated by an expected DAS usability issue: the difficulty of accurately duplicating sketches whose lines cross near grid lines or grid line intersections. It is named for the ancient board game Go, which involves strategically placing tokens on the intersection points of a grid. In Pass-Go, users draw their password using grid intersection points (instead of grid cells in DAS). The user's movements are snapped to grid-lines and intersections, eliminating the impact of small variations in the trace.

A grid-based system resembling a mini Pass-Go has also been deployed commercially for screen-unlock on Google Android cell phones. Pattern Lock [10], a similar system, is available for the Blackberry. Rather than entering a 4-digit PIN, users touch-draw their password on a 3 × 3 grid. The Android screen-unlock scheme has been shown to be susceptible to "smudge attacks", where attackers can determine a user's password through the finger smudges left on the smart phone's surface [11].

2) RECOGNITION-BASED SYSTEMS

Recognition-based systems, also known as *Cognometric systems [1]* or *Search metric systems* generally require that users memorize a portfolio of images during password creation, and then must recognize their images from among decoys to log in.

PASS FACES

The recognition-based system studied most extensively to date is Passfaces [7]. Users pre-select a set of human faces. During login, a panel of candidate faces is presented. Users must select the face belonging to their set from among decoys. Several such rounds are repeated with different panels. For successful login, each round must be executed correctly. The set of images in a panel remains constant between logins, but images are permuted within a panel, incurring some usability cost. The original test systems had $n = 4$ rounds of $M = 9$ images per panel, with one image per panel from the user portfolio.

The user portfolio contains exactly 4 faces, so all portfolio images are used during each login. The theoretical password space for Passfaces has cardinality Mn, with $M = 9$, $n = 4$ yielding 6561 " 2^13 passwords.

RANDOM IMAGES

In Déjà Vu [8], users select and memorize a subset of "random art" images from a larger sample to create

their portfolio. To log in, users must recognize images belonging to their pre-defined portfolio from a set of decoy images; in the test system, a panel of 25 images is displayed, 5 of which belong to the user's portfolio. Users must identify all images from their portfolio and only one panel is displayed. Images of random art are used to make it more difficult for users to write down their password or share it with others by describing the images from their portfolio. The authors suggest that a fixed set of 10000 images suffices, but that "attractive" images should be hand-selected to increase the likelihood that images have similar probabilities of being selected by users.

CONVEX HULL

In the Convex Hull Click Scheme [15], users select and memorize a portfolio of images, and must recognize these images from among decoys displayed, over several rounds. The images are small icons and several dozen are randomly positioned on the screen. Each panel contains at least 3 of the user's icons. Users must identify their icons, visualize the triangle they form, and click anywhere within this triangle. This design is intended to protect against shoulder surfing, but comes at a cost of longer login times.

3) CUED-RECALL SYSTEMS

Cued-recall systems typically require that users remember and target specific locations within an image. This feature, intended to reduce the memory load on users, is an easier memory task than pure recall. Such systems are also called *loci metric* [1] as they rely on identifying specific locations. This memory task differs from simply recognizing an image as a whole

PASS POINTS

During creation of a Pass Points password, users are presented with an image. A password is a sequence of any $n = 5$ user-selected click-points (pixels) on this image. The user selects points by clicking on them using a mouse. During login, re-entry of the click-points must be in the correct order, and accurate within a system-specified tolerance.

Wiedenbeck et al. [2005b; 2005c; 2005a] conducted three lab-based user studies of Pass Points. Users took 64 seconds to initially create a password, and required an additional 171 seconds of training time on average to memorize their password. Login took between 9 and 19 seconds on average. Login success rates varied from 55-90%, with users returning at different intervals to log in again. User performance was found to be similar on the four images tested, and it was recommended that tolerance areas around click-points be at least 14×14 pixels for acceptable usability

V. IMPLEMENTATION

PAIR BASED AUTHENTICATION

Mobile phones are enhanced with the feature of storing personal and confidential information like passwords and PIN numbers. Thus authentication to these devices has become a need. To satisfy the required, two new authentication techniques named pair based and hybrid are implemented. Both the techniques involve the use of session passwords. Pair based authentication [17] consists of phases like registration, login, grid generation, intersection and verification. In registration phase, user enters his username and password. One constrain that has been imposed in this phase is the length of the password. Password length is restricted to 8 since as the length increases, degree of usability decreases. Next is the login phase, where the user enters his username. As soon as the username is entered the password is retrieved from the database (SQLite) based on the username given and a 6*6 grid containing alphabets and numbers is formed using this password. With the grid in the grid generation phase, user has to enter the session password based on the secret pass. The user is supposed to segment his password in terms of character pairs. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Later in the verification phase, session password is verified by comparing the row and column of the intersection character against the pairs of the secret pass. This 6*6 grid interface dynamically changes with no repetition. For every login the grid gets randomized, so that the session password changes for every session.

HYBRID BASED AUTHENTICATION

Hybrid authentication [16] is similar to pair based with a contrast that, it involves the use of both colors and grid of numbers. Hybrid authentication consists of phases like rating the colors, login, grid and color palette generation and verification.

During registration phase, user provides ratings or ranking (1 -8) to colors. User can remember the rating given to colors using some concepts or stories. In login phase, an interface is displayed. The interface consists of 8X8 number grid in which numbers from 1 to 8 are placed haphazardly. In addition to this, a color grid is also displayed containing 4 pairs of colors. Both these grids changes for every session. After a successful registration, user forms a number sequence. This number sequence depends upon the position of the colors in the color grid. User then performs pairing on this sequence of numbers and based on this pairing,

session password is generated. Verification phase of hybrid based authentication is similar to that of pair based authentication.

VI. RESULT

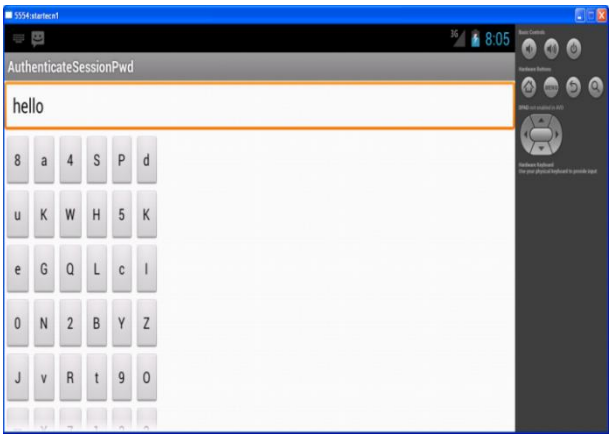

Fig. 1 : Pair Grid Generation

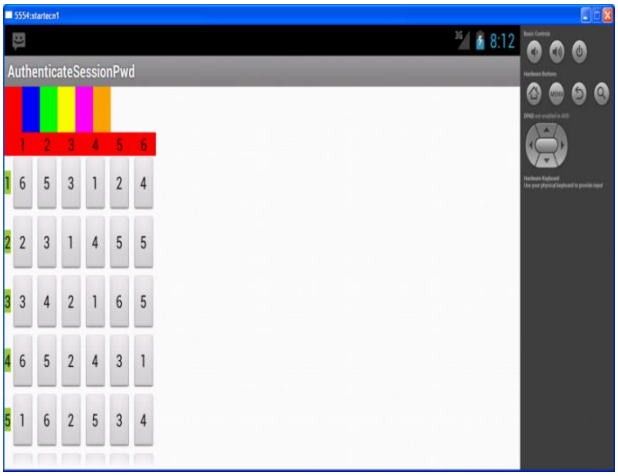

Fig. 2 : Hybrid Grid Generation

VII. CONCLUSION

Though passwords possess their own benefits, still they suffer from various attacks. We have presented an alternate approach to password entry, based on session method which prevents wide range of these attacks.

VIII. REFERENCES:

[1] De Angeli, A., Coventry, L., Johnson, G., and Renaud, K. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies

[2] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. 1999. The design and analysis of graphical passwords. In 8th USENIX Security Symposium.

[3] Goldberg, J., Hagman, J., and Sazawal, V. 2002. Doodling our way to better authentication (Student poster). In ACM Conference on Human Factors in Computing Systems (CHI).

[4] Varenhorst, C. 2004. Passdoodles: A lightweight authentication method. MIT Research Science Institute.

[5] Tao, H. and Adams, C. 2008. Pass-Go: A proposal to improve the usability of graphical passwords, International Journal of Network Security

[6] Renaud, K. 2009a. Guidelines for designing graphical authentication mechanism interfaces. International Journal of Information and Computer Security

[7] Passfaces Corporation. 2009. The science behind Passfaces. White paper, http://www.passfaces.com/enterprise/ resources/white papers.htm.

[8] Dhamija, R. and Perrig, A. 2000. Déjà Vu: A user study using images for authentication. In 9th USENIX Security Symposium.

[9] Wallace Jackson, android apps for absolute beginners, apress, second edition

[10] Tafasa. 2010. Pattern lock. http://www.tafasa.com/patternlock.html.

[11] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., and Smith, J. M. 2010. Smudge attacks on Smartphone touch screens. In USENIX 4th Workshop on Offensive Technologies

[12] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. 2005a. Authentication using graphical passwords: Basic results. In 11th International Conference on Human-Computer Interaction (HCI International).

[13] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. 2005b. Authentication using graphical passwords: Effects of tolerance and image choice. In 1st Symposium on Usable Privacy and Security (SOUPS).

[14] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. 2005c. Pass Points: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63, 1-2, 102–127.

[15] Wiedenbeck, S., Waters, J., Sobrado, L., and Birget, J. 2006. Design and evaluation of a Shoulder-surfing resistant graphical password scheme. In International Working Conference on Advanced Visual Interfaces (AVI).

[16] Authentication Schemes for Session Passwords using Color and Images. In International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011

[17] http://en.wikipedia.org/wiki/Android_%28 operating_system%29#Security_and_privacy

[18] http://www.sqlite.org/

[19] Wallace Jackson, Android Apps for Absolute Beginners, Apress, Second Edition

[20] http://developer.android.com/guide/ developing/index.html

[21] http://www.vogella.de/articles/ AndroidSQLite/article.html

◈◈◈