Graphical Passwords Authentication Using Cued Click Points

Ms. M.Surya [1], Ms.R. Ahila [2]
[1]*PG Scholar*
Department of Computer Science and Engineering
Coimbatore Institute of Technology
Coimbatore.

[2]*Assistant Professor*
Department of Information Technology
Faculty of Engineering
Avinashilingam University For women
Coimbatore.

Abstract

There are many graphical password schemes have been proposed as alternatives to text-based password authentication. It provide a comprehensive overview of published research in the area, covering both usability and security aspects, as well as system evaluation. The first catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. Then it review usability requirements for knowledge-based as they required to apply for graphical password, identifying of security threats of such systems must address and review known attacks.

Index terms
Security and Production, Authentication, Graphical user interfaces, Usable Security.

1.Introduction

A multitude of graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge based authentication mechanisms where users enter a shared secret as evidence of their identity. Where text passwords involve alphanumeric and special keyboard characters. The idea behind Graphical password is to leverage human memory for visual information, shared secret information being related to images or sketches. Despite the large number of options for authentication [4],[5], text passwords remain the most common choice for many reasons. They are easy and inexpensive to implement are familiar to all users essentially all users, allow users to authenticate themselves while avoiding privacy issues that have been raised about

biometrics. However, text passwords also suffer from both security and usability disadvantages for example, passwords are typically difficult to remember, and are predictable if user-choice is allowed.

One proposal to reduce problems related to text passwords is to use password managers. These typically require that users remember only a master password. They store (or re-generate) and send on behalf of the user the appropriate passwords to web sites hosting user accounts. Ideally the latter are generated by the manager itself and are stronger than user-chosen passwords[6].However, implementations of password managers introduce their own usability issues that can exacerbate security problems, and their centralized architecture introduces a single point of failure and attrac- tive target: attacker access to the master password provides control over all of the user's managed accounts.Usability issues often significantly impact its real-world security. User interface design deci- sions may unintentionally sway user behaviour towards less secure behaviour. Successful authentication solutions must thus also include improved usability design based on appro- priate research taking into account the abilities and limita- tions of the target users. In graphical passwords, human memory for visual information is leveraged in hope of a re- duced memory burden that will facilitate the selection and use of more secure or less predictable passwords, dissuading users from unsafe coping practices. This paper provides a comprehensive review of the graphical and reflect on it. It is clear that the graphical nature of the schemes does not by itself avoid the problems typical of text passwords.

Module Description

Registration Phase

The rapid growth in the volume of available information is making it difficult for users to quickly locate pertinent information. Users come from a range of different backgrounds with varied computer literacy and Internet skills, and these users have a wide range of interests and preferences. One particularly important set of Internet users is the business community, who arguably has limited resources in terms of their available time and effort. So to identify users independently, they are registered initially.

Click Point generate phase

Create a password by clicking on one point in each of five system-selected images presented in sequence. an observer sat with each participant throughout the session, noting any difficulties or unexpected behavior as well as comments made by the participants. to create their password and then were progressively quicker in entering it during the Confirm and Login phases

User Substantiate phase

Confirm this password by re-entering it correctly. Users incorrectly confirming their password could retry the confirmation or return to Module 1. A new password started with the same initial image, but generally included different images thereafter, depending on the click-points. Participants said that confirming the password helped them to remember it. Once they had successfully confirmed the password, logging on even after the

distraction task was relatively easy. Participants were extremely accurate in re-entering their passwords. As a measure of accuracy, all individual click-points in the Confirm and Login phases were evaluated.

Alternate Recovery Phase

Answer two 10-point Likert-scale questions on the computer about their current password's ease of creation and predicted memorability. Likert-scale questions ask respondents to indicate their level of agreement with the given statement on a scale ranging from strongly agree to strongly disagree. Participants completed two sets of Likert-scale questions. Ten-point Likert scales were used, where 1 indicted strong disagreement a 10 equalled strong agreement with the given statement. First they answered two online questions immediately after successfully confirming each of their pass- words. They gave both "ease of creating a password" and "ease of remembering their password in a week".

Bolting and Discretization phase

Log in with their current password. If users noticed an error during login, they could cancel their login attempt and try again. Alternatively, if they did not know their password, they could create a new password, effectively returning to Step 1 of the trial with the same initial image as a starting point. If users felt too frustrated with the particular images to try again, they could skip this trial and move on to the next trial. A Discretization method is used to determine a click-point's tolerance square and corresponding grid. For each click-point in a subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point.

Robust Discretization:

This approach involves using three offset grids to guarantee that every point in the image is a "safe" distance away from the edges of at least one grid. It was shown that three grids were necessary and sufficient to guarantee that for any given point in a 2-dimensional space, the system:1) "guarantees the acceptance of approximately correct passwords", i.e., if a login click-point is within distance r from the original click-point then the input is accepted; and, (2) "guarantees the rejection of significantly wrong passwords": if a login click-point is at a distance greater than r_{max} from the original click-point for some specified tolerance, the input is guaranteed to be interpreted as different from the original click-point.

Parameter r represents the minimum tolerance level desired. To achieve the stated objectives, the three grids are diagonally offset from each other by a distance of $2r$ and each grid-square is of size $6r$x$6r$. When an original click-point is selected, a grid is chosen such that the click-point falls at least distance r from the grid's edges. We say that the user-entered click-point is *r-safe* in this particular grid.

When creating a password, a Robust Discretization system selects one of the three grids for each click-point. More specifically, for each point, the system stores. the grid identifier in the clear, and determines which grid-square contains the click-point. The coordinates of this grid-square are cryptographically hashed and the hash is stored along with the grid identifier. For each click-point in future login

attempts, the system overlays the pre-selected grid onto the image and finds the coordinates of the grid-square containing the click-point. The resulting password is hashed to see if it matches the stored hash value.

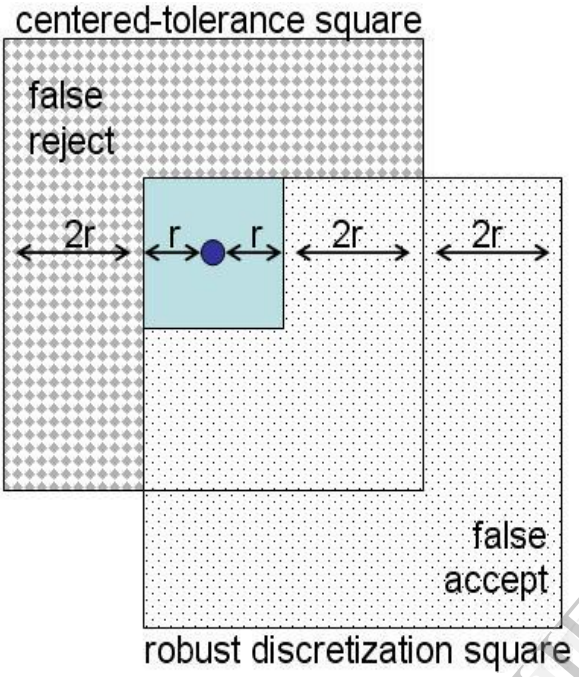

Fig.1. Centered tolerance and robust discretization square.

Centered Discretization:

It offers centered-tolerance, which increases security because the size of grid squares can be reduced , thereby increasing the password search space without negatively impacting usability since the same minimum tolerance is guaranteed. It further increases usability by behaving in accordance with users' likely mental models and eliminating false rejects and false accepts. We first introduce Centered Discretization in 1-dimension and then show how it can be expanded to 2-D for click-based graphical passwords or to higher dimensions.

To understand the severity of false rejects and false accepts in practice, we implemented both Robust Discretization and Centered Discretization to analyze a large data set containing coordinates of passwords and login attempts for these passwords on a PassPoints system.

False Accepts And False Rejects:

With Centered Discretization, the rate of false accepts and false rejects is zero by definition since centered-tolerance implies that the system will only accept click-points that are within *r* from the original point. With Robust Discretization, false positives occur when a click-point is accepted by the system but falls outside of the centered-tolerance grid square of the original point. Conversely, false negatives occur when a click-point falls within the centered-tolerance grid square of the original point but is rejected by the system.

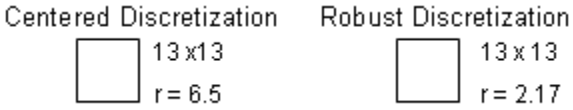

Fig.2.When the grid-square sizes are kept constant, *r* (the minimum guaranteed tolerance) is larger for Centered Discretization.

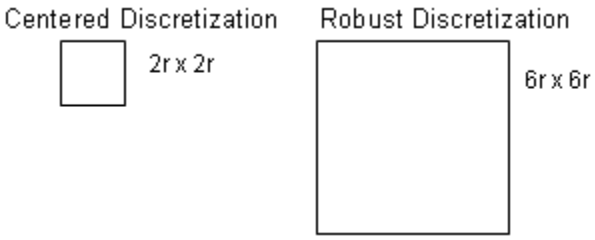

Fig. When *r* is kept constant, the grid-squares for Centered Discretization are smaller, so the password search space is

larger.

There are two approaches to measuring false negatives and false positives. The first is to assume that the Centered Discretization square is the same size as the Robust Discretization square (see Figure 5), but the Robust Discretization square may not be centered on the click-point. It shows the percentage of passwords that would have been falsely accepted and falsely rejected with Robust Discretization, with tolerance squares of the same size as Centered Discretization. For example, using the dataset as described in Section 4 with a tolerance square of 13x13 pixels, 21.1% of passwords are falsely rejected during login using Robust Discretization, but would have been accepted by Centered Discretization using a 13x13 grid. This indicates serious usability issues if a click-based graphical password scheme was implemented using Robust Discretization, since more than a fifth of passwords were falsely rejected.

The second approach is to keep parameter *r* constant rather than the size of tolerance squares (see Figure 6). This means that the minimum guaranteed tolerance around a click-point is kept constant between Centered Discretization and Robust.

Discretization, but it also means that the Robust Discretization squares are much larger than the Centered Discretization squares. For this comparison, there can be no false rejects in Robust Discretization because everything within *r* is guaranteed to be accepted. However, the larger squares required by Robust Discretization lead to false accepts. For example, with *r*=6, 14.1% of passwords are falsely accepted as correct in our dataset.

Result Analysis And Discussion:

Click-based graphical passwords have been proposed as a more usable and more secure alternative to text passwords. Usability testing of such systems so far has been conducted using a centered-tolerance discretization approach and Robust Discretization may well make them less usable. Our results suggest that this would be the case, but since our analysis was conducted post hoc, it is unknown whether users of a Robust Discretization system would resort to some kind of compensatory behaviour. This still indicates usability issues however, since users would be responsible for coping with the system's behaviour.

We present the first analysis of how the usability and security of click-based graphical passwords are affected by the type of discretization implemented. We identified weaknesses in Robust Discretization that lead to false rejects and false accepts, which we expect makes the system appear unreliable from the users' point of view. To compensate, Robust Discretization must use larger tolerance squares, which reduces the password space considerably, making it more susceptible to attack. Centered Discretization guarantees centered-tolerance, increases the password space since smaller grid squares can be used, and makes graphical passwords more usable in real systems by making system behaviour more predictable since the tolerance square is centered on the original click-point (avoiding false accepts and false rejects).

We provide evidence of the usability and security of both schemes by analyzing data collected from a large user study of PassPoints.

Conclusion

Graphical passwords offer an alternative to text-based passwords that is intended to be more memorable and usable because graphical passwords rely on our ability to more accurately remember images than text.Several forms of graphical passwords have been proposed. The system allows user choice while attempting to influence users to select stronger passwords. It also makes the task of selecting a weak password (easy for attackers to predict) more tedious, in order to discourage users from making such choices.

References

[1] Robert Biddle, Sonia Chiasson, P.C. van Oorschot School of Computer Science Carleton University Graphical Passwords: Learning from the first twelve years.

[2] F. Alsulaiman and A. El Saddik. A novel 3D graphical password schema. In IEEE Int. Conf. on Virtual Environments, Human-Computer Interfaces and Measurement Systems, July 2006.

[3]J.Anderson andG. Bower. Recognition and retrieval processes in free recall. Psychological Review, 79(2):97–123, March 1972.

[4] M. Anderson and J. Neely. Memory. Handbook of Perception and Cognition, chapter 8, pages 237–313. Academic Press, 2nd edition, 1996.

[5] F. Monrose and M. Reiter. Graphical passwords. In L. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 9, pages 157–174. O'Reilly Media, 2005.

[6] D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K.Mammi. Towards identifying usability and security features of graphical password in knowledge based authentication technique. In Second Asia International Conf. on Modelling & Simulation, pages 396–403. IEEE, 2008.

[7] K. Renaud. Guidelines for designing graphical authentication mechanism interfaces. International Journal

[8] A. Narayanan and V. Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In ACM Conference on Computer and Communications Security (CCS), November 2005.

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

[10] M. Backes, M. Durmuth, and D. Unruh.Compromising reflections or how to read LCD monitors around the corner. In IEEE Symposium on Security and Privacy, 2008.

[11] S. Chiasson, R. Biddle, and P. C. van Oorschot. A second look at the usability of click-based graphical passwords. In ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

[12] K. Bicakci, M. Yuceel, B. Erdeniz, H. Gurbaslar, and N. B. Atalay. Graphical passwords as browser extension: Implementation and usability study. In Third IFIP WG 11.11 International Conference on Trust Management, Purdue University, USA, June 2009.

[13] G. Blonder. Graphical passwords. U.S. Patent 5,559,961, 1996.

[14] J. Birget, D. Hong, and N. Memon. Graphical passwords based on robust discretization. IEEE Transactions on Information Forensics and Security, 1(3):395–399, 2006.