Towards Secure Design Choices for Implementing Graphical Passwords

GJCST Classification
D.4.6.K.6.5

Machha.Narender[1] M.Y.Babu[2] M.Mohan Rao[3]

***Abstract*-Access to computer systems is most often based on the use ofalphanumeric passwords. However, users have difficultyremembering a password that is long and randomappearing.Instead, they create short, simple, and insecurepasswords. Graphical passwords have been designed to tryto make passwords more memorable and easier for people touse and, therefore, more secure. Using a graphicalpassword, users click on images rather than typealphanumeric characters.. In this paper we describe theDAS(Draw-A-Secret) scheme, its security characteristics,and the empirical study we carried out comparing DAS toalphanumeric passwords. In the empirical study participantslearned either an alphanumeric or graphical password andsubsequently carried out three longitudinal trials to inputtheir passwords over a period of five weeks. The results showthat the graphical group took longer and made more errorsin learning the password, but that the difference was largelya consequence of just a few graphical participants who haddifficulty learning to use graphical passwords. In thelongitudinal trials the two groups performed similarly onmemory of their password, but the graphical group tookmore time to input a password.**

I. INTRODUCTION

Until recently computer andnetwork, security hasbeen formulated as a technical problem.However, it is now widely recognized that mostsecurity mechanisms cannot succeed withouttaking into account the user (Patrick, Long, &Flinn, 2003).. A key area in security research isauthentication, the determination of whether auser should be allowed access to a given systemor resource. Traditionally, alphanumericpasswords have been used for authentication, butthey are known to have security and usabilityproblems. Today other methods, includinggraphical passwords, are possible alternatives.This paper reports on research aimed to design anew kind of graphical password system,empirically test its usability, and compare it toalphanumeric passwords. The significance of thisresearch is the provision of a flexible graphicalpassword system with extensive human factorsdata to support it.We refer to the security and usability problemsassociated with alphanumeric passwords as "thepassword problem" (Wiedenbeck, Waters,Birget, Broditskiy & Memon, 2005). Theproblem arises because passwords are expectedto comply with two fundamentally conflictingrequirements:

1) Passwords should be easy to remember, and the user authentication protocol should beexecutable quickly and easily by humans.
2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

This problem has led to innovations to improvepasswords. One innovation is graphicalpasswords, i.e., passwords that are based onimages rather than alphanumeric strings. The basic idea is that using images will lead togreater memorability and decrease the tendencyto choose insecure passwords. This, in turn,should increase overall password security.Several graphical password systems, described in the next section, have been developed and someHCI evaluation has been done.

II. BACKGROUND ON PASSWORDS

A. Problems with Alphanumeric Passwords

The password problem arises largely from limitations of humans' long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. Decay and interference explain why people forget their passwords. Items in memory may compete with a password and prevent its accurate recall (Wixted, 2004). If a password is not used frequently it will be even more susceptible to forgetting. A further complication is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing passwords. Users typically cope with the password problem by decreasing their memory load at the expense of security. First, they write down their passwords (Adams & Sasse, 1999). Second, when they have multiple passwords, they use one password for all systems or trivial variations of a single password. In terms of security, a password should consist of a string of 8 or more random characters, including upper and lower case alphabetic characters, digits, and special characters. A random password does not have meaningful content and must be memorized by rote, but rote learning is a weak way of remembering (Rundus, 1971). As a result, users are known to ignore the recommendations on password choice. Two recent surveys have shown that users choose short, simple passwords that are easily guessable, for example, "password," personal names of family members, names of pets, and dictionary words (Sasse et al., 2001; Brown, Bracken, Zoccoli, & Douglas, 2004). To users the

About-[1]Assistant Professor ,HITS College of Engineering.
(e-mail-machha.narender@gmail.com)
About-[2]Assistant Professor,Aurora Engineering College
(e-mail- mannavababu@gmail.com)
About-[3]Assistant Professor Tirumala Engg College
(e-mail-mohanrao19@yahoo.com)

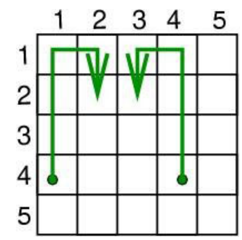
most important issue is having a password that can be remembered reliably and input quickly. They are unlikely to give priority to security over their immediate need to get on with their real work.

B. Why Graphical Passwords?

Graphical passwords were originally described by Blonder (1996). In his description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. Memory of passwords and efficiency of their input are two key human factors criteria. Memorability has two aspects: (1) how the user chooses andencodes the password and (2) what task the user does when later retrieving the password. In a graphical password system, a user needs to choose memorable locations in an image. Choosing memorable locations depends on the nature of the image itself and the specific sequence of click locations. To support memorability, images should have semantically meaningful content because meaning for arbitrary things is poor (Norman, 1988). This suggests that jumbled or abstract images will be less memorable than concrete, real-world scenes. LTM does not store a replica of the image itself, but rather a meaningful interpretation (Mandler & Ritchey, 1977). To retrieve the locations a user will be dependent on the encoding used while learning. A poor encoding will hurt retrieval by failing to distinguish similar objects. Depending on the graphical password system, at retrieval time users will be presented with either a recognition task or a cued recall task. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known.
Recognition is an easier memory task than pure, unaided recall (Norman, 1988). In our password system we use an intermediary form of recollection between pure recall and recognition, cued recall. Scanning an image to find previously chosen locations in it is cued recall because viewing the image reminds, or cues, users about their click areas. Psychologists haveshown that with both recognition and recalltasks, images are more memorable than words orsentences (Sheperd, 1967; Paivio, Rogers &Smythe, 1972; Standing, 1973). This isencouraging in terms of memory for graphicalpasswords.Efficiency is important in password systemsbecause users want to have quick access tosystems. The time to input a graphical passwordby a highly skilled, automated user can bepredicted by Fitts' Law (1954). The law statesthat the time to point to a target depends on thedistance and size of the target ‐ greater distanceand smaller targets lead result in slowerM performance. Existing evidence suggests thatalphanumeric passwords may be faster to inputthan graphical passwords (Dhamija & Perrig,2000). However, the question remains how bigthe difference may be.

III. PROCEDURE TO IMPLEMENT

Drawing a password on a grid.
Passwords are a series of strokes, separated by ―pen-up" events.
Picture maps to a sequence of (x, y) points (e.g. (1,4), (1, 3), (1,2), (1,1), (2,1), (2,2)).
Strength in temporal order.
Length is the sum of the number of cells in each stroke (excluding pen-ups), e.g. 12 in diagram to right.
Stroke-count is the number of strokes in a password (e.g. 2).



A. Important points

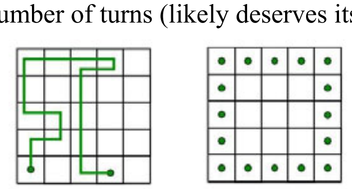
Motivation: Gain understanding of how certain parameters we call password complexity properties affect the security of graphical passwords (to aid in better design choices, password rules, and mnemonics).
We identify a set of complexity properties based on a set of pattern complexity factors from Attneave [1].
We refer to passwords that minimize their complexity properties to be probable passwords, belonging to the probable space.

B. Results

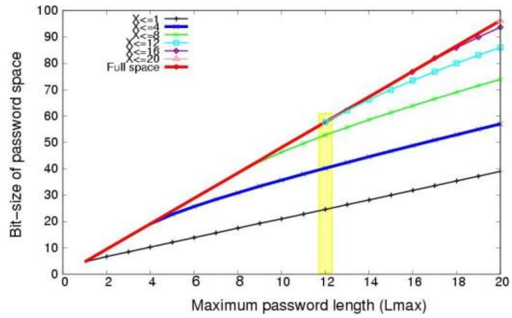
We identified a complexity property with a significant impact on the password space: strokecount, X.Larger impact than other complexity properties.Evidence users will choose low X (e.g. 4).We look at ways to increase security of graphicalpassword implementations in light of theseresults.
The graphical password scheme we examined(DAS). Our definition of graphical passwordcomplexity properties. Results of examiningcomplexity properties in relation to DAS.Methods to increase the DAS password space.Security implications and recommendations.Parameters that we hypothesize would adverselyaffect memorability, which we call complexitypropertiesIn textual passwords, these factorscould be length, and the amount of numbers,special characters, etc

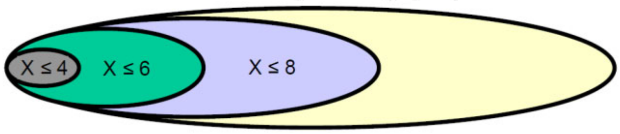
A. Complexity Properties Identified

We identify a set of complexity properties basedon a set of visual pattern complexity factors from
Attneave:
Password-length
Stroke-count.
Symmetry (examined in previous work).
Number of turns (likely deserves its own study).



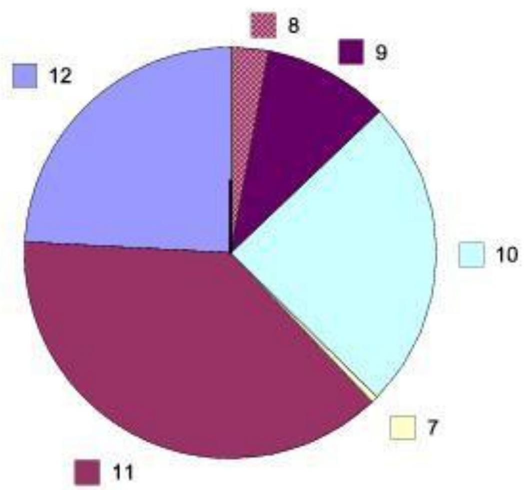
B. Maximum Stroke-count(X) and Length





C. Stroke-count (X)

12 dots (24%), 10 dots, 1 line (38%)
Proportion of password space attributable to passwords consisting of exactly *X* strokes.
Here *Lmax = 12*, on a 5 by 5 grid.
Note that for 6 or fewer strokes, the proportion is so small it is not visible

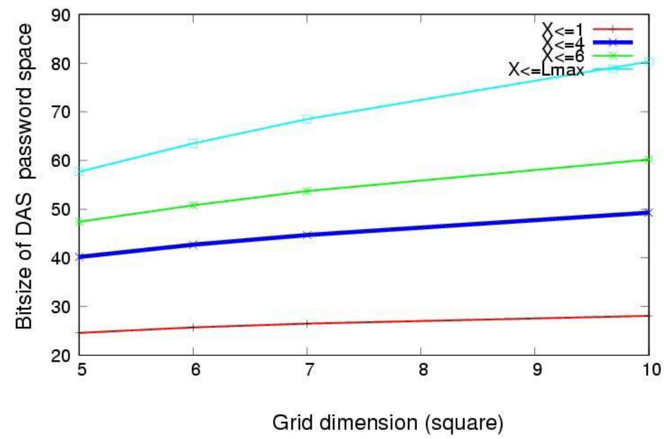


D. Security implications

These values are for Lmax=12, 5 by 5 grid.
X = stroke-count.
Key point is relative times.
We think X ≤ 4 is more representative of what users would choose.

Password set	Time to exhaust(1CPU-32GHz)
Full DAS	541.8 Years
X<6	157.1 Days
X<4	1.1 Days
X<1	1.9 Seconds

E.Increasing DAS's Password Space -Increasing Grid size



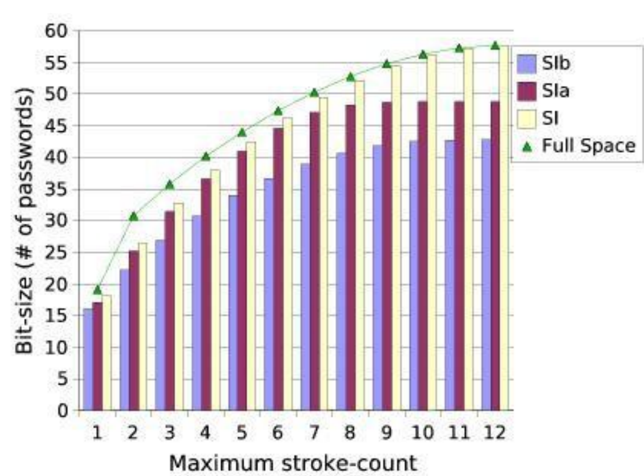
In the above graph, Lmax = 12. Less thanexpected increase achieved, especially when X ≤ Lmax/2.

Password now becomes a combinationof the drawing grid chosen, and thedrawing itself. Amount of extra security achieved depends on selection grid size, and minimum/maximum accepted drawing grid dimensions.e.g. 30 by 30 selection grid, minimum 5, maximum 10 grid dimension provides 16 bits

F. Resulting Recommendations

DAS Password rules:
At least one stroke of length 1.
A stroke-count of at least Lmax/2.
Avoid global symmetry (Usenix Security 2004).
Implementation decisions:
Increasing grid size provides low payback if users choose passwords with a low strokecount (likely).
Grid selection (or related variation) should be implemented to increase the DAS space.

G. Summary of Current Knowledge



IV. Future Work

Alternate encodings for DAS to increase size of password space (and decrease number of passwords "disallowed"). A better understanding of the breakdown of what users have the most difficulty recalling, leading to a more formal definition of complexity properties. Perhaps sacrificing the most difficult to recall parts of DAS to encourage users to choose more strokes would be useful (e.g. direction of strokes). Password set Time to exhaust(1CPU-32GHz) Full DAS 541.8 Years
X<6 157.1 Days X<4 1.1 Days X<1 1.9 Seconds Psychology studies to see how parameters such as stroke-count and temporal order affect memory. Stroke-count is the complexity property with the largest impact on DAS's password space. A more viable attack strategy for DAS passwords than previous work. Secure design choices in implementations: Grid selection instead of simple grid size increase. Password rules: user guidelines and proactive checking.

V. References

1) Adams, A. and Sasse, M.A. (1999). Users are notthe enemy. Communications of the ACM 42, 12,41-46.
2) Birget, J.C., Hong, D., and Memon, N. (2003).Robust discretization, with an application tographical passwords. Cryptology ePrint Archive.http://eprint.iacr.org/2003/168 accessed January17, 2005.
3) Blonder, G.E. (1996). Graphical Passwords.United States Patent 5559961.Boroditsky, M. Passlogix password schemes.http://www.passlogix.com, accessed December2, 2002.
4) Brostoff, S. and Sasse, M.A. (2000). ArePassfaces more usable than passwords: A f ieldtrial investigation. In McDonald S., et al. (Eds.),People and Computers XIV - Usability or Else,Proceedings of HCI 2000, Springer, pp. 405-424.
5) Brown, A.S., Bracken, E., Zoccoli, S. andDouglas, K. (2004). Generating andremembering passwords. Applied CognitivePsychology, 18, 641-651.
6) Dhamija, R. and Perrig, A. (2000). Deja Vu:User study using images for authentication. InNinth Usenix Security Symposium.
7) Fitts, P.M. (1954). The information capacity ofthe human motor system in controlling amplitudeof movement. Journal of ExperimentalPsychology, 47, 381-391.
8) Mandler, J.M. and Ritchey, G.H. (1977). Longtermmemory for pictures. Journal ofExperimental Psychology: Human Learning andMemory, 3, 386-396.
9) Morris, R. and Thompson, K. (1979). Passwordsecurity: A case study. Communications of theACM, 22, 594-597.
10) Norman, D.A. (1988). The Design of Everyday Things. Basic Books, New York.