Volume 2, No. 5, May 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

TECHNICAL NOTE

Available Online at www.jgrcs.info

PASSWORD IN PRACTICE: AN USABILITY SURVEY

Naveen Kumar
Assistant Professor, School of Computer and Information Sciences,
IGNOU, Maidan Garhi, New Delhi, 110068, India.
Email: naveenkumar@ignou.ac.in

Abstract: User Authentication is the process of determining whether a user should be authorized to access to a particular system or resource. Alphanumeric passwords are most common mechanism for authorizing computer users, even though it is well known that users generally choose passwords that are vulnerable to dictionary attacks, brute force attack and guessing attacks. Until recent years, the security problem has been formulated as a scientific problem. However, it is now extensively accepted that security is also a human computer interaction (HCI) problem. Most security mechanisms cannot be effective without taking into account, the user. HCI matters in two ways. One is the usability of the security systems themselves and another is the interaction of the security systems with user practices and motivations. We have studied the usability of alphanumeric passwords, and found that they are more difficult for people to remember and the consequence is that one has to write them down. We have discussed the usability versus security tradeoffs and found different inherent weaknesses in alphanumeric passwords. We have also discussed the alternative solutions those can be used instead of alphanumeric password.

Keywords: User Authentication, Password, Security, usability.

INTRODUCTION

Through the advancements and versatility of Internet, password protected accounts are very common and widely used for a variety of online applications including instant messaging, personal and business e-mail, online banking, online ticket booking and shopping accounts. Due to sensitivity of the user information within these accounts and possibilities of misuse of this information by others, we expect that users would create very secure passwords. However, it is well known that people normally choose passwords using meaningful words that are easy to remember, using a proper name or using a word commonly found in the dictionary, that are vulnerable to dictionary attacks [1]. For example, in one case study of over 14,000 UNIX passwords, almost 25% of the passwords were found by searching for words in a dictionary [2]. The security and usability problem associated with alphanumeric passwords is referred as “The password problem”[3]. The password problem arises because passwords are expected to comply with two fundamentally conflicting requirements.

1. Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by human beings.
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.

Satisfying these requirements is virtually impossible for users. Consequently, users ignore the requirements, leading to poor password practices. Most schemes are dependent on unique user name/password technique with some limitations and restrictions. For example, passwords must be at least eight characters long and must contain at least two non-letter characters; they must also be changed at least once a month.

Many of the limitations of alphanumeric password schemes occur due to the limited capacity of human memory. In case human beings are not required to remember the password, a maximally secure password would be one with maximum entropy.

It meant it can have a password consisting of a string as long as the computer can process, consisting of all characters supported by the computer system, and in a manner that provides no redundancy. This problem is well acknowledged in the security world. The previous studies by Morris and Thompson in the year of 1979 [4], and Feldmeier and Karn in 1990 [5] have shown that, normally users tend to choose and handle alphanumeric passwords very insecurely. Moreover, the current studies by Brown et al. in 2004 [6] also confirm the results of previous studies.

The result shows that the alphanumeric passwords have drawbacks, most notably in terms of memorability and security. This led to the necessity to improve alphanumeric passwords. One such improvement is graphical passwords, i.e. passwords that are based on pictures or images rather than simple alphanumeric strings. The primary reasoning is that, using images will lead to greater memorability and decrease the tendency to choose insecure passwords, as human being’s ability of visual memory is much more powerful than the textual memory [3][7][8].

SURVEY

To understand the applicability, scope and nature of the user authentication problems and towards improving the security of user authentication, we conducted a research to study password-based security, particularly to investigate password memorability and the problem of forgetting passwords, alternative authentication scheme, usability and security of alphanumeric passwords. A survey was developed to investigate and expand on information regarding a diverse range of specific user practices, the extent of knowledge users have and use in the construction and use of passwords. These issues combined with five usability goals were used to evaluate text based and image based authentication [9]. The survey is divided into two studies: The first is to understand the weakness of alphanumeric schemes, and the second is to explore the memorability issue of alphanumeric passwords.

Study 1

Study 1 tests a methodology and estimates some of the basic parameters of alphanumeric password system performance in a real world setting. These parameters include:

1. Number of passwords owned and Content of passwords (proportion containing numbers and symbols) / password strength.
2. User behaviours towards secure password practices, password length (number of characters), ease of recall of passwords, frequency of use of passwords and frequency of problems with passwords, type of problem with passwords.
3. Internet usage behaviours (frequency, duration and longevity of use), types and number of different password-protected accounts maintained, actual practices used in generating, storing and using passwords.
4. Understanding the practices used in generating and storing passwords.

Study 2

To collect information about the users performance with alphanumeric passwords, during the creation session and recall session, two questionnaires were designed. The parameters for study 2 are as follows:

1. Actual practices used in generating, storing and using alphanumeric passwords.
2. Investigate importance of the number of passwords owned by users as a factor, and to investigate the factors influencing password system performance.

Survey Participants

A total of 202 teachers, staff and university students from Indira Gandhi National Open University, New Delhi and Jamia Millia Islamia, New Delhi volunteered to participate in the survey, and were regular users of computer and Internet with one or more password protected accounts. Ages of the participants ranged from 17 to 61 years; 76% were male participants, and 24% were female. Seven cases were removed due to improper and missing data, resulting in 195 participants in the final data analysis.

EVALUATION PROCEDURE

We conducted a questionnaire-based survey. The overall survey was divided into three parts as explained in the following sections.

Part 1: Alphanumeric Passwords

The first questionnaire was relevant to the alphanumeric password, their performance and user behaviour towards these password schemes. It also covered the demographic information. However, in this name was an optional field to help user write about his usual mistakes and problems frankly without hesitation.

Part 2: Password Creation Phase

Part 1 and Part 2 questionnaires were given to user one after another. In part 2, users were asked to create two alphanumeric passwords according to the standard password policies. The password policies and requirements were provided to the user as both verbal and written instructions. Users were not allowed to reuse any previous or current password that they used. In addition, users were not allowed to use a variant of a password that were then in use or had been previously used. The user was advised to not provide any personally identifiable information in their password.

Part 3: Password Verification Phase

In this verification phase, users were asked to recall and create two alphanumeric passwords that they had created seven days ago during the Part 2 of feedback study.

EVALUATION RESULTS

This section presents the statistics in graphical representation using MS-Excel software. Important results are shown phase wise against the question asked to the user in respective questionnaire.

Part 1: Alphanumeric Passwords

Question. How many personal passwords do you have for Emails, websites and computers? Please estimate to the best of your ability.

Result: To know the memorability issues we asked participants to give the number of passwords they are using. More than 60% of our participants (as given below in figure 1) had more than six passwords, and might have been suffering from 'The Password Problem'. As the number of passwords increases the memorability problem also increases. We found that only 8% participants had more than 11 passwords.

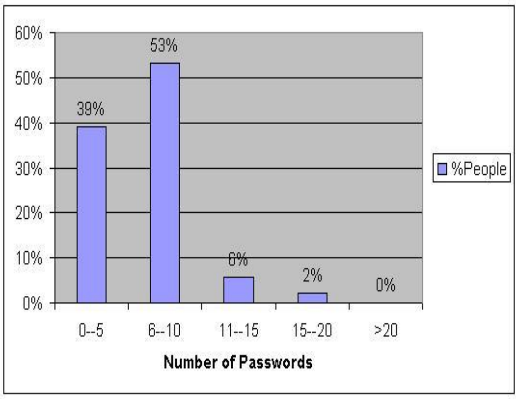

Figure 1: Number of Participants' Passwords

Question. How often do you change your passwords?

Result: Further, to find out bad password practices, we also found that large groups of regular computer users were not following good password policies, as shown in figure 2, Only 18% users were changing their password at least in a month, however this result has not considered the password policy and restrictions enforced by websites, banks, and administration.

We found that 67% of users were not changing their passwords or changing them annually.

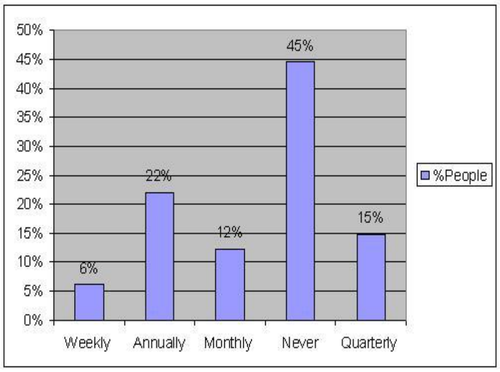

Figure 2: Frequency of Changing Passwords

Question. If you do change your passwords, do you switch it back to an old password? (Please check one response.)
Result: As shown below in figure 3, large group of people (79%) was exactly reusing their passwords, which is more evident of bad password practice.

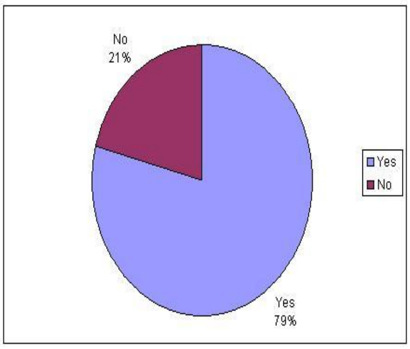

Figure 3: Response on Switching Back to an Old Password

Question. Do you use same password for different Emails, websites and computers?
Result: The figure 4 given below shows that only 30% of users are keeping different passwords for different accounts. However, again, this result reconfirms the fact studied by other researchers that users use same password for different accounts. We assume that to avoid the inconvenience of access to services and memorability problem, in combination, lead the users to adopt bad password practice.

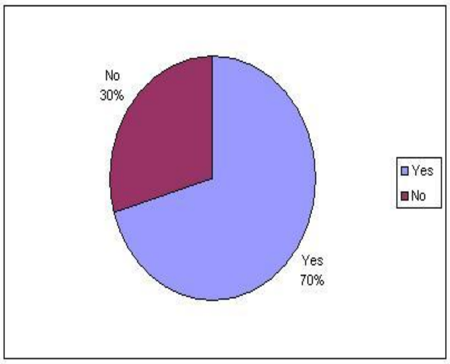

Figure 4: Response on Keeping Same Password for Multiple Accounts

Question 5. How many times in the last six-month have you forgotten any of your passwords?

Result: As given below in figure 5 below, 66% of the users had forgotten their password atleast once in six months; however 20% had lost it for atleast 5 times. This established the fact that users are suffering from 'The Password Problem'. However, 15% of users had not answered for this question.

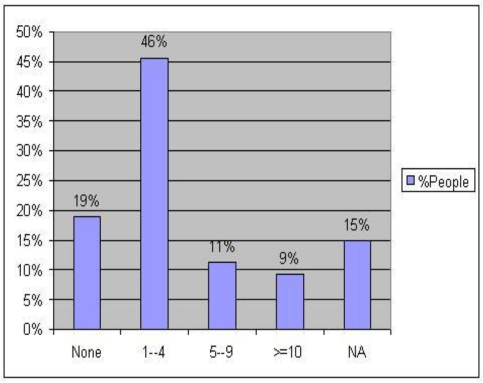

Figure 5: Number of Times Participants Have Forgotten Password

Question. How did you choose your password? Were you inspired by any of the following sources? (Please check all that apply.)

□ Name of celebrities
□ Name of Family Members
□ Literature (book, poetry, etc.)
□ Scientific or other educational mnemonic
□ Familiar Numbers (street address, employee number, telephone number, birth date, etc)
□ Personal experience
□ Other (please specify):_________________

Result: The user inspirations for creating password (given figure 6), it shows that this tendency of users leads to easy hacking, cracking and guessing of their passwords. Most users use their family details in their passwords. However, next inspiration for people is celebrities and literature. Specialized dictionary for command names; celebrities and literatures can create easy password hacking attempts. Around 14 responses gathered from some participants took other inspirations like car and bike names, their numbers, pet names, favourite colours, favourite dresses, favourite food and places, for their passwords (these are similar to the sources given in our question).

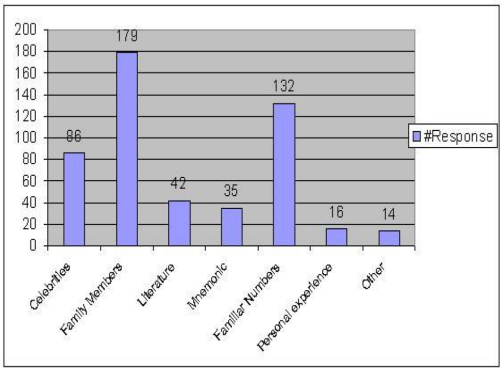

Figure 6: Sources of Password Inspiration that Participants Use

Question. When you create your new password, which of the following factors do you consider? (Please check all that apply.)

□ Does not contain dictionary words
□ Is in a foreign (non-English) language
□ Is not related to the site (i.e., the name of the site)
□ Includes numbers
□ Includes capital letters
□ Includes special characters (e.g. "&" or "!")
□ Are at least eight (8) characters long
□ None of the above: I didn't think about it
□ Other (please specify)________________

Result: The result in figure 7 given below gives an idea of the users' awareness about good password policies. From the large responses that were collected, most of them keep eight letters password including numbers, which sound encouraging. However, this result may be affected by the restriction given by the network administrators and websites. Only in nine responses, participants admitted that they cared about the password restrictions. Also, only 98 participants tried to keep a password that is not available in the dictionary.

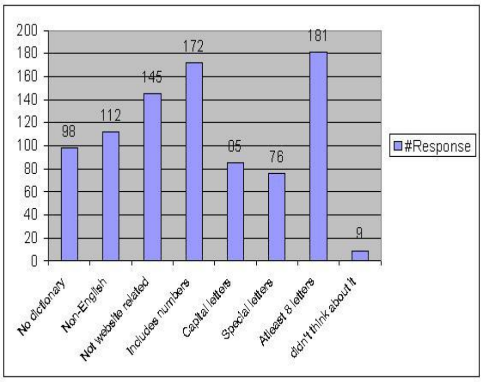

Figure 7: Factors Considered by Participants during Password Creation

Question. Has anyone ever broken into an account of yours (bank, email, work, etc.) by stealing, guessing, or cracking your password?

Result: As given in figure 8, most of the participants (78%) say that no one had broken into their account (bank, email, work, etc.) by stealing, guessing, or cracking their password. 16% participants don't know about it, and only 6 % had encountered such experience. However, as the Internet shopping, banking and trading is increasing in India, there is a probability of increase in password threats.

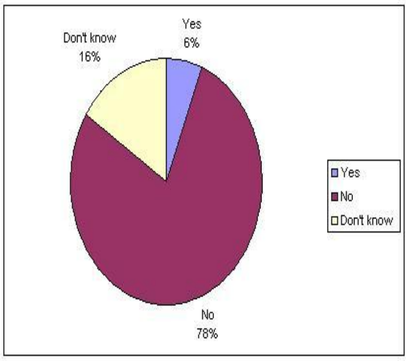

Figure 8: Response of Participants on Password Hacking

Question 9. How do you remember all of your passwords? (Check all that apply.)

□ Write on paper (notebook, day planner)
□ Try to remember (Human Memory)
□ Use computer file (Word document, Excel sheet, text file etc)
□ Store in Mobiles or PDA
□ Encrypted Computer File (e.g. CryptoPad)
□ Use Password Software (Password Agent, Password Tracker etc)
□ Website Cookies (Website checkbox: "Remember my password on this computer")
□ Web Browser (Internet Explorer AutoComplete)
□ Password Reminder (Website feature: "Forgot your password?")
□ Other (please specify) _______________

Result 9: The safest way of storing password is user's own memory. In 174 responses, users have responded of using the same password for multiple accounts. A large section of participants use paper or computer unencrypted files for storing their passwords (refer to figure 9). However, we got eight responses in which participants used encrypted file and six responses in which they used password manager software (interestingly for these softwares participants again have to remember other passwords). Web auto- complete and websites cookies are also used by many participants, which are very unsafe methods.

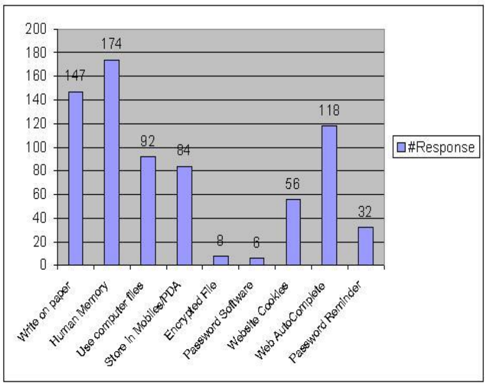

Figure 9: Ways of Remembering Passwords

Question. Have you ever used a computer program to generate your passwords?

Result: In attempt for proving safe passwords, many computer programs are available, which can automatically generate passwords for the users. However, the seed value used is again questionable. Only 5 % participants were using these softwares, and 33% are not aware of it. As shown in figure 10, 62% of the participants were not using it, which indicates that the users either doubt or feel inconvenient with these programs.

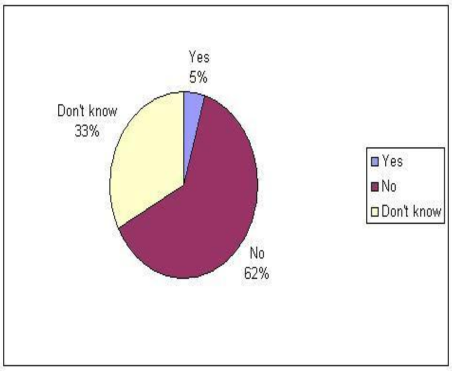

Figure 10: Response of Participants on Password Generating Programs

Question. Think back the last time when you created a user account. How did you choose the password for this account? (Please check all that apply.)

□ Reused a password that is used elsewhere
□ Modified an existing password
□ Randomly generated a new password
□ Created a new password based on a name (your name, your significant other's name, your pet's name, etc.) or a date
□ Picked a word and changed it (added numbers, capital letters, etc.)
□ Picked a memorable phrase, and used a character to represent each word in the phrase
□ Other (please specify) _______________

Result: The user behaviour about creating a new password is given in figure 11. Results show that participants either used same password (156 responses) or modified the currently used password (133 responses). Comparatively, lesser number of participants (only 115 responses) created new password.

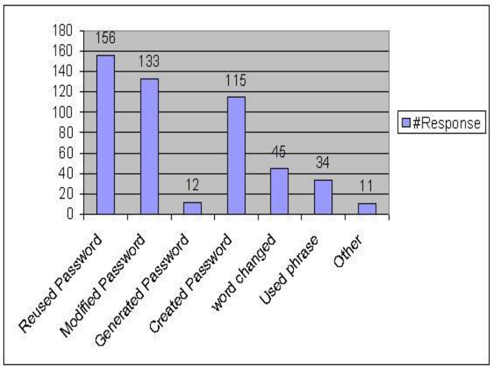

Figure 11: Response of Participants on New Password Creation

Part 2: Password Creation Phase

Question. Except alphanumeric password, which of the following user authentication mechanism you have used? (Please check all that apply.)

□ Mnemonic phrase based password
□ Smart card with PIN (e.g. ATM cards)
□ Fingerprint scanning
□ Voice based password
□ Graphical Passwords
□ None
□ Other (please specify)_____________

Result: Almost all participants were familiar with smart cards (ATM cards) as shown in the figure 12 given below. Further, 76 responses have used mnemonic phrase based password. This indicates that, as users are comfortable for adopting alternative user authentication methods. Although, ATM cards or Smart cards are also affected by the password problem [4].

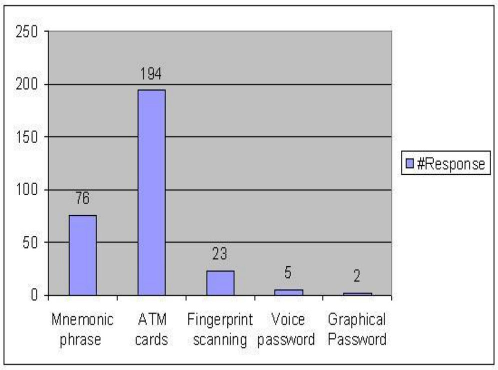

Figure 12: Participants Familiarity with Different Authentication Methods

Question. How confident are you that you can learn two new alphanumeric passwords, and remember them a week later, without writing them down?

Result: After creating the alphanumeric passwords, 75% of participants were confident of recalling it after seven days (Figure 13). However, only 17% of them were actually able to recall it. The reason behind this contradiction in the confidence shown and the actual behaviour is possibly the habit and immaturity of creating week alphanumeric password.

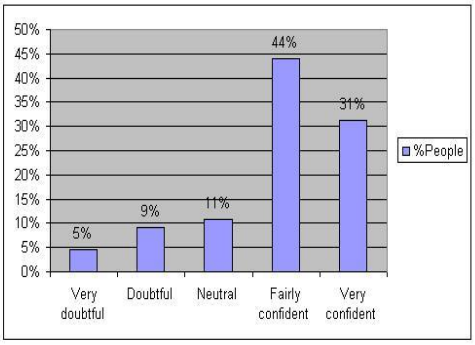

Figure 13: Participants' Confidence towards Alphanumeric Authentication

Part 3: Password Verification Phase

During the password creation phase, we had asked participants to create two alphanumeric passwords, considering the fact that most of the people have to remember multiple passwords. However, for verification and evaluation purpose we took only the data of first password in both cases.

Question. Please recall and write exactly the passwords, which you had created seven days back, in the boxes.

Result: Out of 195 participants, only 104 were able to create an alphanumeric password with password policies (In spite of written and oral clarification to the participants). Among these, 83 % participants failed to recall the password correctly (only 17% were successful in recalling the password correctly). The remaining 91 participants out of 195 participants created password without minimum requirements. However, 40% of participants had recalled their password successfully as given in figure 14. This result shows that the usability and security are conflicting requirements.

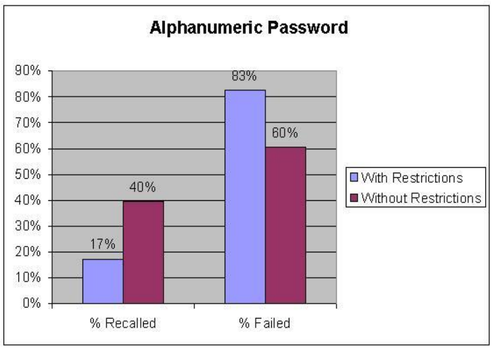

Figure 14: Participants' Memorability towards Alphanumeric Passwords

CONCLUSION

Overall, the evaluation of survey results suggested that most of the users were not able to implement good password policies and that the users are facing password problem. However, due to the unavailability and acceptability of alternative authentication schemes, users had to opt for other non-secure mechanisms like website auto-complete feature and cookies. Our primary hypothesis is that experienced and inexperienced users deviate from the secure model of behaviour in different ways. Specifically, experienced users have multiple passwords but tend to write them down, while inexperienced users have a single password but do not write them down. In addition, we believe that users have adopted their own password management schemes, which often involve using the same password for multiple web sites. We did not expect to find significant correlations with age or gender, although this information was gathered.

We presented a set of questionnaire-based model for evaluating the Security & Usability of alphanumeric passwords, particularly, to investigate memorability of alphanumeric passwords. We presented the results based on a diverse group of users. We had validated the facts found in some of the prior work in this area. Moreover, we had also point out some of the inherent limitations of alphanumeric passwords. We recommend that other user authentication schemes like fingerprint authentication and graphical password could be emerged as an alternative to the alphanumeric password. Our survey evaluation is probably not representative of the Internet population. The survey on larger set of participant may be conducted through website conversion of the questionnaires.

REFERENCES

[1] Australian Computer Emergency Response Team, 2004, Computer Crime and Security Survey, Queensland University, Brisbane, Australia.

[2] Klein D, 1990, Foiling the cracker: a survey of, and improvements to, password security, proceedings of the second USENIX Security Workshop.

[3] Wiedenbeck S., Waters J., Birget J. C., Brodskiy A., and Memon N, 2005, PassPoints: Design and longitudinal evaluation of a graphical password system, International Journal of Human Computer Studies, Vol 63, pp. 102-127.

[4] Morris, R. and Thompson, K., 1979, Password security: a case study, Communications of the ACM 22, pp. 594–597.

[5] Feldmeier, D.C. and Karn, P.R, 1990, UNIX password security-ten years later, In Advances in Cryptology-CRYPTO'89. Lecture Notes in Computer Science 435, Springer, Berlin, pp. 44–63.

[6] Brown, A.S., Bracken, E., Zoccoli, S., and Douglas, K., 2004, Generating and remembering passwords, Applied Cognitive Psychology 18, pp 641–651.

[7] D. Bensinger, 1998, Human memory and the graphical password, Passlogix, White Paper.

[8] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., and Rubin, A.D., 1999, The design and analysis of graphical passwords, In proceedings of the Eighth USENIX Security Symposium, pp. 1-14.

[9] Brostoff, S. and Sasse M.A., 2000, Are Passfaces more usable than passwords: a field trial investigation, People and Computers XIV-Usability or Else, Proceedings of HCI, Springer, Berlin, pp. 405–424.