Password Construction and Management Strategies of the Online Users of Bangladesh: A Demographic Comparison with the Users of the First-World Countries

S M Taiabul Haque
Department of CSE
University of Texas at Arlington
Texas, USA
Email: eresh03@gmail.com

Tauhidul Alam
Department of CSE
Chittagong University of Engineering & Technology
Chittagong, Bangladesh
E-mail: tauhid_cuet@cuet.ac.bd

Mamoon-Al-Rasheed
Department of CSE
State University of Bangladesh
Dhaka, Bangladesh
Email: mamoon@sub.edu.bd

Matthew Wright
Department of CSE
University of Texas at Arlington
Texas, USA
E-mail: mwright@cse.uta.edu

***Abstract*—In this paper, we report on a study of the password construction and management strategies of advanced online users in Bangladesh. The study involved a survey of 75 undergraduate Computer Science students from two different universities. Their responses suggest that even these advanced online users are not aware of some generally accepted good password practices. Our findings are also compared with the responses of various user studies that have been conducted among the users in first-world countries. The Bangladeshi users in our study, who have fewer passwords than first-world users, are more likely to write down passwords and share passwords less frequently. They also do not change their passwords regularly. On the other hand, users in our study generate passwords with fewer personally meaningful words and numbers than first-world users, and a majority of our participants do not use common English or Bengali words. The study is the first of its kind in Bangladesh and it highlights the key weaknesses in the password management strategies of these advanced online users.**

Keywords—Password, usable security, user study, demographic comparison

I. INTRODUCTION

In the present age of computer and information technology, creating and maintaining an online account has become an important task. A user needs to create an online account in a website for the purpose of being exclusively identified by that website. This online account gives the user a unique identity, through which the user can interact with the website authority or other users. An online account acts on behalf of a user in today's digital world and the identity of a user can easily be compromised by compromising any important online account of that user. Therefore, the security and protection of an online account is of paramount importance. In most of the cases, this security relies upon remembering and protecting a sequence of characters, which is also known as password.

Although other forms of authentication mechanism exist, password-based authentication is considered to be the most cost effective one. Several researchers have proposed biometric authentication schemes by exploiting fingerprints [1], retina of eye [2], or voice properties [3]; but their implementations require a lot of expenses. Passwords can be graphical and textual but graphical password schemes have limited deployment in real world. Graphical password schemes like hand-drawn doodle passwords [4] or image-based passwords [5] are not as popular as textual passwords due to the simplicity associated with the use of textual passwords.

Textual passwords, however, are not free from limitations. A good textual password needs to be an easy-to-remember and a hard-to-guess sequence of characters [6], which sometimes presents a dilemma. Because words that are easy to recollect from memory are generally single and short words that can be found in a standard dictionary. If this kind of word is chosen as a password, the password becomes susceptible to dictionary attacks [7], which attempt to guess a password by systematically entering every word in a dictionary as a password.

This password management problem is aggravated when a user needs to maintain multiple password-protected accounts. A recent study revealed that on average, a user of a first-world

country maintains 25 password-protected accounts [8]. On the other hand, in an earlier work, it was reported that the cognitive capacity of an average user restricts the user from dealing with more than four or five passwords effectively [9]. As a result, an average user uses the same password for multiple accounts. This habit is called "password reuse" and if a user reuses a password across multiple accounts, a hacker gaining access to one of the accounts may also be able to compromise other accounts. So, reusing the same password across multiple accounts opens the door for cyber criminals for exploiting a user. This "domino effect of password reuse" has been discussed in detail in [10].

Apart from password reuse, users also follow other poor password practices. Survey results have reported that users write down their passwords on a piece of paper for the convenience of remembering them [11], they frequently share passwords with other people [12], and they use personally meaningful words or numbers that are easily guessable [13]. Due to the lack of consciousness of users, security experts now acknowledge that: "..security is only as good as it's weakest link, and people are the weakest link in the chain." [14]. As a result, numerous user studies have been conducted by modern cyber security researchers to explore the underlying human factors of computer security; and a contemporary branch of security has evolved, which is known as "usable security".

In this study, we conducted a survey among the users of Bangladesh in order to get an overview of their password practices. To the best of our knowledge, this is the first academic study conducted in Bangladesh about password practices of users. We compared the responses of our survey with the responses of the surveys that have been conducted among the users of the first-world countries and highlighted the key weaknesses in the password management strategies of the users of Bangladesh.

The rest of the paper is organized as follows. In Section II, we describe the methodology of our study. We present our findings in Section III. Section IV discusses about the implications of our findings. We summarize our key findings and highlight about future research direction in Section V.

II. METHODOLOGY

We conducted an online survey with 31 undergraduate students (22 male, 9 female) of a private university located in Dhaka (the capital and the largest city of Bangladesh) and 44 undergraduate students (39 male, 5 female) of a public university located in Chittagong (the second largest city of Bangladesh).

The survey was conducted through Survey Monkey. Survey Monkey is a website that helps to administer online surveys. We conducted a pilot study among five students first. The pilot study revealed that the students felt more comfortable if the questions were asked in Bengali, their mother language. Therefore, in the actual survey, we asked the questions in Bengali. But we also provided the English translation for each of the questions and for all the answer options.

The survey consisted of ten questions. Questions were asked about the frequency of password-protected accounts, password reuse strategy, password sharing habit, languages used while creating a password, frequency of changing passwords, and password construction and management methods. All of the questions were closed-ended multiple choice questions. We used a 5-point Likert scale (1=Never, 2=Seldom, 3=Sometimes, 4=Often, 5=Always) for some of the questions. Demographic questions were included at the end of the survey. For privacy and security reasons, we only asked the participants about their gender and age. We did not ask for any personally identifiable information like name or email address. In this way, we ensured the privacy and security of the participants of our survey. The students did not receive any direct benefit (money or extra course credit) for participating in the survey. However, we told them that by participating in our survey, they would be able to understand their own password behavior more clearly.

One of the main objectives of our study was to compare between the password practices of the users of Bangladesh and the users of the first-world countries. Therefore, we sought a study population that is as web-savvy as average Internet users of the first-world countries. Therefore, we conducted our study among the Computer Science majors. These users should possess more online accounts than an average user of Bangladesh and they should also be more conscious about the security of their online accounts. By limiting our study sample to Computer Science majors only, we tried to make the comparison as fair as possible.

III. RESULTS

We now present our major findings from the survey. Three of the participants did not complete the survey and we did not consider their responses in our results.

A. Number of Password-protected Accounts

Since it is really hard for a participant to count the exact number of his/her password-protected online accounts, we asked the participants to specify the range. The responses of the participants are shown in Table I.

B. Password Reuse Habit

When the participants were asked about their password reuse habit, their responses suggested that they frequently reuse a

TABLE I: NUMBER OF PASSWORD-PROTECTED ONLINE ACCOUNTS

Number of Accounts	Number of Participants
Less than 5	22
5 to 10	24
11 to 15	11
16 to 20	3
Greater than 20	12

TABLE II: REASONS CITED FOR PASSWORD REUSE

Reason	Number of Participants
I have too many accounts	3
It is easier to remember	37
I reuse the same password for the accounts of same category	6
I only use one password for all of my accounts	3
I reuse the same password for all unimportant accounts	7
I never reuse the same password for multiple accounts	16

password for multiple accounts. Only 22.2% (16 out of 72) of participants reported that they "never" reuse a password for multiple accounts. On the other hand, 8.3% (6) reported that they "seldom", 41.7%(30) reported that they "sometimes" and 19.4% (14) reported that they "often" reuse a password. Surprisingly, 8.3%(6) of participants reported that they "always" reuse a password for multiple accounts.

The participants were also asked to cite the reason for reusing a password. Their responses are summarized in Table II.

C. Password Construction Language

Participants were specifically asked whether they use English words/phrases in their passwords or they construct their passwords by using Bengali words/phrases. We also gave them a third option "While creating my password, I use random words/phrases more that are not associated with a specific language (for example – abd123, asdf etc.)".A majority of the participants (37 out of 72) selected this third option. On the other hand, only 37.5% (27) of participants reported that they use English words/phrases, while only 11.1% (8) of participants reported that they use Bengali words/phrases. This revealed an important implication about the password security of the users of Bangladesh. This issue is discussed in detail in Section IV.

D. Password Sharing Habit

We asked the participants how frequently they share their Facebook or email passwords with friend and family. Almost 80% of participants (70.8% said "never", 8.3% said "seldom") indicated that they do not share passwords. This suggested that password sharing is not a widespread habit among the users of Bangladesh.

E. Password Construction Methods

Since we were interested to know about the password construction methods of the users, we specifically asked the participants what practices they follow while constructing a password for an important account. We gave them a series of six practices and asked them which of the practices they follow. The responses of the participants are summarized in Table III. The first four practices were related with the concept of the bit strength of passwords. The bit strength of a password can be calculated as $\log_2((\text{alphabet size})^{\text{length}})$ [8].

TABLE III: FACTORS CONSIDERED WHILE CREATING A PASSWORD (MULTIPLE RESPONSES ALLOWED)

Practices	Frequency
I use both capital and small letters	32
I use digits	33
I use special characters	23
I create a password longer than 7 characters	36
I use personally meaningful words (school name, birthplace name etc.)	16
I use personally meaningful numbers (age, birthdate, student id etc.)	15

Here, the alphabet size is the sum of the sizes of the different types of characters that are used in a password. These types and sizes are lowercase letters (26), uppercase letters (26), digits (10), and special characters (22). Thus, the bit strength of a password increases if more uppercase letters, digits and special characters are used in that password. The bit strength also increases with the increase of the length of the password. For example, an eight character password that contains both uppercase and lowercase letters and special characters would have bit strength $\log_2(74^8) \approx 49.68$.

The time that is required to crack a password by a password cracker is related to the bit strength of that password. A password that has higher bit strength (a long password with a combination of uppercase and lowercase letters, digits and special characters) is considered to be a good password. It is harder for a password cracker to crack that password because the password cracker would require generating and testing more unique permutations for cracking that password.

It can be seen from Table III that 44.4% of participants of our study reported that they use capital letters and 45.8% of participants reported that they use digits in their important passwords. The frequency of using special characters is comparatively low. About 31.9% of participants reported that they use special characters. However, exactly half of the participants reported that they create a password longer than seven characters for an important account. These findings suggested that for an important account, most of the users create a password that has a reasonably high bit strength.

The last two practices are related with personal experiences and preferences (Table III). The responses of the participants suggested that most of them do not use personally meaningful words (school name, birthplace name etc.) or numbers (age, birthdate, student id etc.) while creating an important password.

F. Frequency of Changing Passwords

We asked the participants how frequently they change their passwords. Table IV shows their responses.

For this question, we allowed the participants to give their own answers. Seven of the participants wrote their own answers. Four of them indicated that they do not have any specific time duration for changing their passwords, while three wrote that they only change their passwords in case of emergencies (spam or virus attacks) or if they feel that their passwords have been stolen.

TABLE IV: FREQUECNY OF CHANGING PASSWORDS

Frequency of Changing Passwords	Responses
Never	24
Weekly	3
Monthly	6
Every three months	7
Every six months	10
Yearly	15

G. Password writing habit

The participants were also asked about the habit of writing down their passwords. Most of the participants revealed that they do not write down their passwords on a paper or in a computer file for the convenience of remembering them. Writing down the passwords on a piece of paper or in a computer file is a bad habit because the paper or the file may get into wrong hands. More than half of the participants (37 out of 72) reported that they "never" write down their passwords on a piece of paper or in a computer file and 20.8% (15) reported that they "seldom" do so. On the other hand, 20.8% (15) and 2.8% (2) reported that they "sometimes" and "often" write down their passwords, respectively. Only three participants reported that they "always" write down their passwords on a paper or in a computer file.

IV. DISCUSSIONS

We explicitly recruited undergraduate Computer Science majors to participate in our survey. Therefore, we do not claim that our results are the best representation of the general Internet users of Bangladesh. However, as mentioned before, we intentionally recruited participants from a technologically savvy demographic because we wanted to explore the password management strategies of the users who are considered to be more educated about technology than an average Internet user of Bangladesh. Our results reflected a best-case example of the users of Bangladesh. It identified the poor security practices that are followed by the users who are relatively more knowledgeable about Internet security and privacy. Our survey results demonstrated that even these users are not well-aware of some of the good password practices. The general Internet users of Bangladesh cannot be expected to be more conscious than this sample population. Our results, therefore, suggest that pragmatic steps should be taken to make the users of Bangladesh more security-concerned about password management strategies.

Our study also highlights several important demographic issues. A recent study from Microsoft Research showed that on average, an Internet user of a first-world country has 25 password-protected accounts [8]. Compared to that, advanced Internet users (Computer Science majors are considered as advanced Internet users because there should be easy Internet access in their labs and they should spend more time on computer/Internet than ordinary users) of Bangladesh have fewer password-protected accounts (Table I).

Although the users of Bangladesh have fewer password-protected accounts and they need to deal with fewer passwords, their password reuse rate is not drastically different from the users of the first world countries. A recently conducted study in Carnegie Mellon University reported that more than 80% of the participants reuse a set of passwords for different accounts [11]. Our survey responses indicated that almost 70% of participants (41.7% said "sometimes", 19.4% said "often", and 8.3% said "always") reuse the same password for multiple accounts.

The users of Bangladesh write down their passwords more frequently than the users of the first world countries. Overall, 51.4% of participants of our study reported that they "never" write down their passwords on paper or electronically, while 87% of participants of the study of Carnegie Mellon University reported that they "do not" write down their passwords [11].

Regarding the habit of password sharing, the users of Bangladesh follow this habit less frequently than the users of the first-world countries. According to a recently conducted study by a researcher of Nokia Research Center, one third of the users share their personal email password; while a quarter share their Facebook password [12]. On the other hand, almost 80% of participants of our study indicated that they do not share their Facebook or email password with friend and family.

Compared to the users of the first-word countries, the users of Bangladesh less frequently use personally meaningful words and numbers while creating their passwords. Table III shows that only 22.2% of participants of our study reported that they use personally meaningful words, while 20.8% of participants reported that they use personally meaningful numbers. In a similar study that was conducted with the students of Wichita State University, a public university of USA, it was indicated that 54.9% of users use personally meaningful words, while 49.8% of users use personally meaningful numbers while creating their passwords [13]. This demonstrates a good practice that is followed by the users of Bangladesh because if personally meaningful words or numbers are used in a password, the password becomes more guessable by others, especially by the close people because they should be more familiar with the words or numbers that are meaningful to a user.

From the responses of the participants, it was also revealed that when creating a password, most of the users avoid English dictionary words and uses random words/ phrases that are not associated with any specific language. As discussed in Section I, an attacker uses a dictionary or wordlist for successfully performing a dictionary attack. Sophisticated password cracking tools like John the Ripper can assist an attacker in this kind of attack [15]. These dictionaries or wordlists are found for English and most other major languages. The website for the Openwall Project [16], one of the biggest repositories for password recovery utilities, contains wordlists for English and 20 other languages. So, a password is relatively safe if English dictionary words are avoided in that password and the responses of our study

showed that most of the users follow this safe practice of avoiding English dictionary words in their passwords. This suggested that the passwords of most of the users of Bangladesh are less susceptible to dictionary attacks.

V. Conclusion and Future Work

We conducted the first academic study about password behavior among the users of Bangladesh and compared our findings with the findings of the studies that have been conducted among the users of the first-world countries. Our study revealed several important findings:

- Even the advanced Internet users of Bangladesh have fewer password-protected accounts than the average Internet users of the first-world countries.
- Although the users of Bangladesh have to deal with fewer passwords, their password reuse rate is not drastically different from the users of the first-world countries.
- Password sharing is not a widespread habit in Bangladesh as it is in the first-world countries.
- The users of Bangladesh follow the poor practice of writing down their passwords more frequently than the users of the first-word countries.
- Most of the users of Bangladesh do not follow the recommended practice of changing passwords regularly.
- For their important accounts, the users of Bangladesh create passwords that are reasonably strong and they less frequently use personally meaningful words or numbers, which make their passwords less guessable.
- Rather than using English/Bengali dictionary words, most of the users of Bangladesh use random words/phrases that are not associated with a specific language, which in turn make them less vulnerable when dictionary attacks are performed by malicious attackers.

In this study, we presented a general overview of the password habits of the users of Bangladesh. In future works, we will focus more on examining the strengths of passwords that are actually created by the users. We will design experiments that would ask the participants to construct new passwords. Analysis of those passwords might help us to better understand the password construction patterns of the users of Bangladesh.

References

[1] A. R. Roddy and J. D. Stosz, "Finger-features statistical analysis and system performance estimates," Proceedings of the IEEE 85(9), (Sep. 1997), 1390-1421.

[2] C. Marino, M. G. Penedo, M. Penas, and M. J. Carreira, "Personal authentication using digital retinal images," *Pattern Anal. Appl.9,* 1(May 2006), 21-33.

[3] H. –J. Kim, "Biometric is it a viable proposition for identity authentication and access control?," *Computers & Security,* 14(3), 1995, 205-214.

[4] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling our way to better authentication," CHI'02 Extended Abstacts on Human Factors on Computing Systems, 2002, 868-869.

[5] R. Dhamija and A. Perrig, "Déjàvu: A user study using images for authentication," Proceedings of the 9th Conference on USENIX Security Symposium, August 2000.

[6] S. Wiedenbeck, J. Waters, J. -C. Birget, A. Brodskiy, and N. Menon," Authentication using graphical passwords: Effects of tolerance and image choice," Proceedings of the 2005 Symposium on Usable Privacy and Security, July 6-8 , 2005, 1-12.

[7] R. Morris and K. Thompson, , "Password security: a case history", *Commun. ACM 22,* 11 (Nov. 1979), 594-597.

[8] D. Florencio and C. Herley, , "A large-scale study of web password habits", 16th International World Wide Web Conference, May 8-12, 2007, 657-666.

[9] [9] A. Adams and M. A. Sasse, "Users are not the enemy", *Commun. ACM 42,* 12 (Dec. 1999), 40-46.

[10] B. Ives, K. R. Walsh, and H. Schneider, , "The domino effect of password reuse", *Commun. ACM 47,* 4 (Apr. 2004), 75-78.

[11] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Majurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: User attitudes and behaviors", Proceedings of the 2010 Symposium on Usable Privacy and Security, July 14-16, 2010.

[12] J. J. Kaye, , "Self-reported password sharing strategies", 2011 Annual Conference on Human Factors in Computing Systems, May 7-12, 2011, 2619-2622.

[13] S. Riley, "Password security: What users know and what they actually do",*Usability News,* 8(1),2006.

[14] B. Schneier, "Secrets and lies", John Wiley and Sons (2000).

[15] http : //www.openwall.com/john.

[16] http : //www.openwall.com/wordlists.

.