Boosting Authentication Security by Building Strong Password and Individualizing Easy to Remember Techniques

Nooruldeen Nasih Qader

College of Science and Technology
University of Human Development
nooruldeen.qader@uhd.edu.iq

Abstract - Newly released researches disclose the need of canceling the incorrect opinion; security by Password (PW) is dead and proves that these believe has been hurtful. Moreover, recommended a campaign prioritize strategies of building PW. Considering the PW features such as costless, maturity and vast experiences, and usability PW continues to be the most used options in Information Security (IS), it is furthermore, consider most challengers to researchers and really needs further boosting. PWs control authentication mechanism of IS, requiring that individuals choose strong PW. The best advice to protect from hackers is randomly generating unique PW for every site and service, to apply this advice we need more techniques of easy to remember and hard to guess. This study proposed a bunch of easy to remember techniques for building a strong PW. Also, it exhibited the importance of similar strategy despite existing of many helpful PW managers. On the other hand, this paper compiled and analyzed today's data regarding authenticating secure systems via PW. Analyzed data showed some of common weakness in PW selection. Moreover, gathered information and evaluated data indicated the need of boosting PW. Proposed techniques and solutions enable individuals to select appropriate PW easily.

Keywords- Password Manager Authentication Security

Encryption Hacker Usability,

Introduction

Word PASSWORD (PW) could be translating to Personal Account Security System WORD; PW is a string of characters utilized to prove the user identity (i.e., authentication). Moreover, currently, PWs are going to crack to gain unauthorized access to a computer without the computer owner's awareness [21]. The average Web user preserves 25 different accounts, however makes use of simply 6.5 PWs to secure them, suggests that when hackers have plucked login qualifications from one site, they frequently have the ways to jeopardize dozens of other accounts, too [9].

Everywhere in digital life requires a PW to register for something or another. Most of available service online requires registration, also PW required for Wi-Fi, ATM, …etc. in all cases an issue arises on how selecting a new PW? More importantly, how could user remember it? Due to its convenience and ease of PassWord (PW), it is the most popular form of user authentication. Today's Internet services rely heavily on text-based PWs for user authentication. The pervasiveness of these services coupled with the difficulty of remembering large numbers of PWs. Thus, users tempt to reuse PWs at multiple sites. Security protocols have developed at a pace largely matching the development of online threats, but PWs persist in being the same – despite increasing demands on authentication mechanisms [5].

Developing a PW that is both safe and unforgettable gets difficult and harder, the more of them we need to memorize. It is necessary to be able to come up with PWs that are personal sufficient to bear in mind, however, varied and complex adequate to be protected, so finding out the best ways to develop proper PWs is an important ability that you will most certainly use commonly [6].

A good PW is not just restricted by what a human can bear in mind; however, it is likewise restricted by what a person can produce. We can get digits and punctuation into PWs easily enough, however our options techniques involve much predictability. That predictability can be exploited in PW hacker's tools. They are not only checking out the same PW that gets published in locations like this, but they have studied millions of swiped PWs. Here is a vital principle that we need to keep in mind: The strength of a PW production system is not exactly how lots of letters, digits, and symbols you end up with, but exactly how lots of ways you might get a various outcome utilizing the same system (i.e., PW entropy).

We are pursuing better PWs, not best ones. One must take only as many suggestions from this, as s/he comfy with and no more. Remembering and entering the PW should not be a problem [12].

This paper is organized as follows: literature survey followed by adopted techniques to collect required information; information related of today PW practicing. After that, a discussion about balancing between security and usability have displayed followed by PW cracking issue. Section 6 presented a bunch of easy to remember and hard to guise techniques, 24 techniques organized in four venues: PW length, keyboard, substitution, miscellaneous, and master techniques. Today's data regarding using PW are presented in discussion and result section. Finally, the conclusions of the research have presented.

Literature Survey

[17][10] Discussed incorrect assumption that PWs are dead and showed the hazard of such assumption, and declines research to find effective methods to improve using PW and serve around two billion users. Moreover, they demand that every work should be accomplished to correct this. PW mechanism proved as an outstanding to protect assets effectively where used probably, and attempts to replace it has vanished. One of the factors that make replacing PW with any others mechanism is its usability [10]. Using PW was and remains popular, even using PW are ascending increased. The research showed in several cases, PW is the perfect solution.

[18] This paper proposes the strategic framework of multilayer checkpoints for database security, and discusses that a balance between security and simplicity is necessary since both are required. The paper presents authentication via PW as an important layer of security.

[17] Discusses tradition method of authentication, PW still the most common method for identification and authentication due to its easiness and familiarity. Meanwhile, most users practice insecure behaviors in using of PW (e.g., writing down PWs). Thus, PW considers the weakest link in the authentication mechanism, but it could be efficient if selected intelligently and managed properly. However, powerful using of PW requires a PW be simple to remember and not easy to predict. Nevertheless, almost all PW users do not realize security problems. To have a secure information system, developers should direct or even enforce users to follow techniques that guaranty powerful PW.

[16] Address PW security and usability challenge, and proposed a novel PW scheme, called "Travel PW", which is memorable and secure. The proposed scheme is developed to aid users memory by adapting mnemonic devices, e.g., pictures and symbols, and story telling. Mnemonic device aids memory because humans can remember pictures better than text. The paper results shown 90% of users can remember strong PWs in the proposed scheme, compared with 58% of the textual one.

Data Gathering Techniques

In this study, several techniques have been applied to gather related data by using PW; some of these techniques are being discussed in the following:

1. Distributing and collecting questionnaires, which have a specific use in information gathering. The benefit of it is enabling the project team to collect information from a large number of stakeholders. Even if the stakeholders are widely distributed geographically, they can still help collect large quantities of data through questionnaires.

The questionnaire of this study distributed to 1000 IS users and 30% of them have replayed. Collected questionnaires reviewed thoroughly to valid gathered information. The questionnaire obtains insight information about currently using of PW. This information helps to determine the areas that need further research, interviews, and observation. Moreover, it reveals new eras that need more improvement and techniques.

2. Conduct interviews and discussions with users. Interviewing is by far the effective way to understand the obstacles. It is also, the most time and resource-consuming option. In this study, PW users of variety academic levels have interviewed. A list of detailed questions is prepared and discussed. To conduct effective interviews, it organized in three areas: preparing for the interview, conducting the interview and following up the interview.
3. Observe and test, along with interviews, another useful method of gathering information is observation PW user. As a result, wide experiences about using PW in information security were achieved. This first hand-experience is critical to find exactly weak points in PW authentication processes.

Balancing Security Against Usability

PW could be complex, but almost certainly at a great cost of memorability. It had been known since 1990 that people pick weak PWs. To protect important systems with single-factor authentication, the user should change PWs often, but strong PWs may be hard to generate [7][20]. This was the main factor of creating PW manager, PW manager is great for generating strong and random PWs for sites without you ever having to memorize them, but a class of people does not convenience with PW manager [17]. Moreover, there are PWs that need to remember despite utilizing PW manager (e.g., master PW, Wi-Fi, OS, ATM). The user should know how to build strong and memorable PW.

Some other techniques have been built-in with most IS to assist users remembering and recovering PW; such as PW hint, security question, and PW resets, but despite of those techniques our survey demonstrates that users are not well practicing PW (for more detail refer to section 7). Users frequently use some bad manner to recall their PWs such as written down, reuse, not change, weak PW, and share it with other, for details of PW threats you can refer to [17].

There is a trade-off between PW security and usability; longer PW provides higher security, but it may reduce usability (i.e., harder to remember) [16][19]. Here, creating a perfect PW is not a goal; instead looking for a good PW that remain usable. It is a trouble if a user picks a PW that is too difficult to type or too hard to remember. Therefore, always keep in mind that a PW that cannot be typed or remembered is a terrible choice of PW. The sensitivity of accountable judges the required level of strong PW (e.g., master PW, ATM) [8][1].

Today Smartphones are used for typing PW, but they have a limited keyboard. Thus, typing "#3ok;U)9" to connect to a network is time-consuming [11]. Therefore, Stanford University recently announced using schema shown in figure 1. The new Stanford PW standards are balancing between user convenience and security. It may be noteworthy because it depends mostly on PW length rather than entropy [21].

PW CRACKERS

The Kerckhoffs's principle assumes that opponent knows about the system as much as defender knows, thus if the PW user implements security recommendations to produce powerful, easy to remember PWs, the opponent who will trying to break that PW are at least as familiar with that advice as the user are. Some security administrator direct users to take care of PW generator rule. Thus, they do not need to remember hundred PWs if they have one rule set for generating them. One way to generate unique PWs is to choose a base PW and involve a rule that mushes the service name with it. *The risk of such advice is higher because if a hacker catches some PWs they can deduce all others*. The hackers know at least as much about how people pick PWs as we do. Our survey shows that 47% of users reuse the same PW across ten sites (for details refer to section 6). The hackers identify a few simple tricks that users often employ to transform a basic PW between sites which can be used by an attacker to make PW guessing vastly easier [8].

Hackers permeating Gawker servers and exposing cryptographically safeguarded PWs for 1.3 million of its users; botnets were splitting the PWs and using them to commandeer Twitter accounts and send out spam. Then the sites encouraging or requiring their users to alter PWs expanded to include Yahoo, Amazon, and Twitter [23]. "The danger of weak PW habits is becoming increasingly well-recognized," [21].

PW breaking tools are becoming effective every year. The ancient art of PW breaking has advanced further in the past five years than it did in the previous some decade combined.

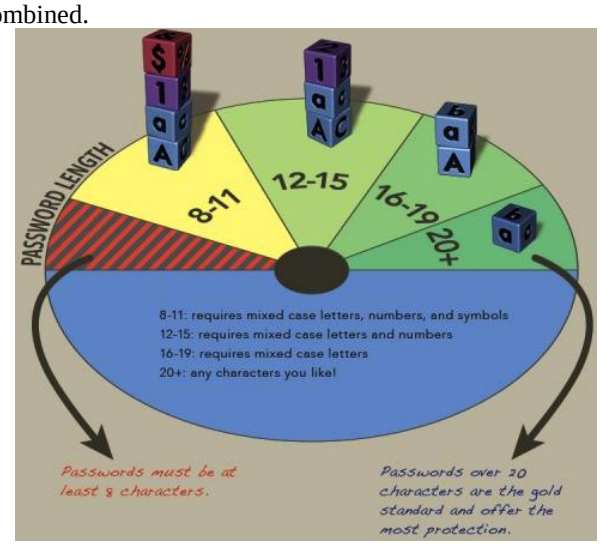

Figure- 1: Stanford PW requirements, last modified April 17, 2014 [15].

Entropy increases the security and guessing of PW, NIST considers that the division of PWs corresponds to an entropy of 4 bits for the first character, 2 bits for the next 7 characters, and 1.5 bits per character for the 9th to the 20th character, and 1 bit per character for the remainder of the PW. 6 bits of entropy are added when the user is forced to use uppercase and non- alphabetic characters. This is for traditional PWs – mobile PWs are likely to have lower entropy due to the complications of entering them. It is also a mode and evidence that users choose PWs of varying toughness of varying kinds of account. Analysis of PWs from raiding drop boxes suggests that the average PW length was 7.9 characters, which corresponds to the entropy of approximately 18 bits. While this indicates that the average probability of guessing a PW is 2^{-18}, popular credentials are attempting by an attacker and consider fruitful to a reasonable amount of accounts [11].

Depending on what sort of access the hackers have, they can test from 1000 PWs per second to hundreds of thousands per second. If some companies are insisting on consuming hundreds of millions of dollars only to discover an individual secret, then one has to not consider the issues manageable only by PW; multifactor security should be used. The best advice to protect from hackers is randomly generated and unique PWs for every site, to apply this advice we need more techniques of easy to remember and hard to guess.

Eight-character PWs- when arbitrarily produced and contained a mix of numbers, symbols, and upper- and lower-case letters- can take months or years to split. That is because the only method that works versus such PWs is to try huge numbers, prospects till the assailant discovers the one that works. The vast variety of possible combinations makes these strength attacks exceptionally hard to perform.

More recent hardware and contemporary techniques have also assisted to contribute to the rise in PW cracking. A PC is running a single AMD Radeon HD7970 GPU, for circumstances, can attempt on typical an astonishing 8.2 billion PW combinations each second, depending on the algorithm made use of to scramble them.

An attacker uses a dictionary file containing about 26 million words, combined with shows guidelines that greatly extend its effectiveness by including numbers, punctuation, and other characters of each list entry. Relying on the task, he sometimes uses a 60 million-strong word list. Presumably choices such as "P@ssw0rd1", which can usually be broken in seconds [3].

EASY TO REMEMBER AND HARD TO GUISE TECHNIQUES

A secure, unforgettable PW is easy to remember, and difficult for others to estimate. In general, most people cannot remember more than seven random characters. A few people can remember 10 or 11 random characters. If the person does not have a systematic manner in which to memorize information, data in short-term memory can be stored up to 30 seconds [4]. Reported that nearly half of the respondents indicated that they wrote down their PWs to aid their PW memorability.

The secret to strong PWs is not choosing a PW, but to build a PW. Do not simply consider some phrase and utilize that as the PW. Apply some specific technique to

create a complex PW that is not only efficient, but also effortless to keep in mind. Here are some techniques for building strong PWs. The approach here adopts a template that is effortless to keep in mind but produce a PW that is less predictable. The overall guidance here is being innovative and use them as styles for personal ideas [2][14].

A. PW Length Techniques

Complex, multi-word PWs are difficult to crack, and they can be just as simple to remember as a short PW.

1. Extend PW Length

One of the rules of strong PW is complexity, and one of the factors that make PW complex is its length. One can use the technique of associate the PW (after building it uniquely) with the current year (e.g., 2014), a website address, or any other thing. The purpose of this technique is only extending the length. Therefore, one may apply other technique(s) to build the PW, and by this technique extends the PW length and in the same time can be easy to remember.

2. Repetition

Consider repeating a simpler PW. Length can easily help the strength of a PW, thus if user wants to apply the repeating method, s/he can select a relatively simpler word and then duplicate it. Thus, s/he will have less to keep in mind, and the PW is going to be strong! It is easier to remember one thing and type it twice or more. Just make sure the user is smart about how he do it. Typing the same thing twice is a common technique and very predictable. Instead, vary how repeating things, e.g., "reallyReally long is reallyreally strong", "I'll...be...back...", "Nowaynohownoone".

3. Base PW

Use base PW with the first two consonants and the first two vowels of the service name. For example, the phrase "east and west" create base PW as "stndwseaae", now the base have ten characters that easy to remember and easy to type and for the sites you use a lot, you will end up memorizing them pretty quickly. Something simpler - but along the same lines - might involve the same base plus the number of a service name and adding the symbol @ increasing the length and entropy of PW. Then the PW for Gmail would be stndwseaae1@Gmail, and the PW for amazon would be stndwseaae1@amazon. If the user is not willing to apply some extra effort to obscuring a rule set and base PW, then just forget it, it is almost worthless.

4. Use Multi-Words

The technique revolves around picking multi-words (e.g., two words) that are relevant enough for the user to recall them easily, but if others recognized one of the words, they could not conveniently predict the other words. Consider including numbers, capitals, punctuation, or other modifications to make the PW even more powerful (e.g., 33 free trees, Walking talking keyring). This pattern allows a user conveniently build PWs of twenty or more characters. Despite that, all have to do is recall a few bits of information about the chosen two words.

The trick to this specific technique is to have one typical factor in each word to assist user recall the PW and to help him in considering of distinct words beyond of personal things or in user surroundings. By selecting words associated with each other in various means, it forces a user to be more innovative. There are numerous ways to link words beyond meaning only [2].

5. Make a Compound Word

An intelligent method to create an easy-to-remember PW is to integrate multi small words that have the personal implication. One can use "mydogspot" instead of "My dog spot" or "jimswifejane" instead of "Jims wife Jane" [1].

6. The E-Mail Address, The Phone Number, The URL

Society has qualified our minds conveniently discover specific templates, so construct PWs to imitate those templates. These always produce great PWs. Among the ideas, is to pattern a PW after a fabricated email address. It is strong PW since it contains a lot of the elements of a powerful secret.

We are frequently shelled with WEB addresses, so why not make use of that and design PWs after that paradigm? (e.g., www.sendallyourmoney.irs.gov). Certainly there is no need to terminate with only a single domain name extension or even legitimate extensions. The further a user get out of the criteria, the more chance he has to raise the entropy of the PW [2].

7. Use What Could be Remembered Easily

Anyone has a massive of things that he can remember easily, these things could be good raw material for building PWs, but the important issue is to build it *smartly*. For example, to build a PW using pai relation, one can write "in_my_math_pai=22/7" or "in_My_maTh_pai=22%7".

Use the existing year and the first three letters of the ongoing month. Moreover, it is easy to include three letters coming from (e.g., an animal name). Within this case, a PW might read 2014mayDeer. Upcoming month, modify it to 2014junJone. It is impractical to get the identical PW two times or to forget it. One can make it more random by employing other techniques such as repeating something, e.g., 201414junJoneJone.

Mix a date element within a larger PW. This aids when the PW has to change from time to time. Keep in mind to never employ just a date, a PW consist only of the date is at higher danger of being cracked than other options [1].

B. Keyboard Techniques

1. Diverse the Selection of Keyboard Positions

Stander keyboard has more than 50 buttons in four rows. So, one can select different PWs by positions as shown in figure 2.

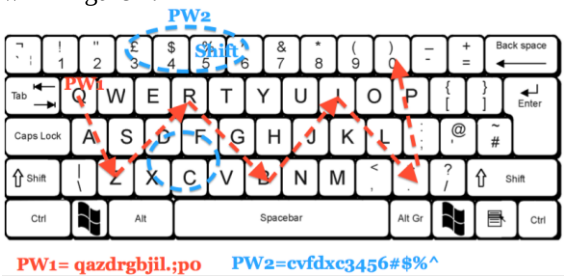

Figure- 2: Build PW based on keyboard position.

2. *Use Shift and Caps Keys With All Techniques*

Powerful PWs consist of lowercase characters, uppercase characters, digits, and symbols. Create a model of pressing shift for the initial three characters, or characters two through five, or whatever a user prefer. Each key has a specific character and with the shift key it has another character. Do not forget to use shift and caps keys with other techniques as shown in figure 3. This makes PW complex and easy to remember, e.g., If one uses PW "bgt098bgt098" for a month s/he can handle first change of this PW only as before, but with holding down shift key it becomes "BGT) (*BGT) (*".

3. *Shift Keys Out of the Normal Typing Position*

If a user PW does not use the Q, A, or Z, s/he can hit the key to the left of the PW. Or to the right if s/he do not use the P, L, or M. Shift right, left, up, or down such that for PW "bestrong" shift right change it to "vwareibf", shift left "nrdytpmh", shift one key up producing "g3w549ht", and one key down " dxgfl b" [1]. Also, one can mix shifts, e.g., shift one key right for first word and shift one key up for a second word, i.e., "bestrong" convert it to "vww549hg". Also, one can shift two keys instead of one key; also s/he can mix all shifting together.

Figure- 3: Using shift with keys for building PW.

4. *Utilize Mobile number or Postal code on The Computer Keyboard*

For number 1 the numbers straight below the 1 key are Q, A, and Z as shown in figure 4. Instantly, for producing a PW, one pushes the first number that he selected, and then pushes all of the character keys that are straight below it. Then all he has to keep in mind are the numbers. If he desire a more challenging PW, attempt capitalizing the first character of the row, making one of the digits a symbol (e.g., 5→ s), or anything else with those lines [1].

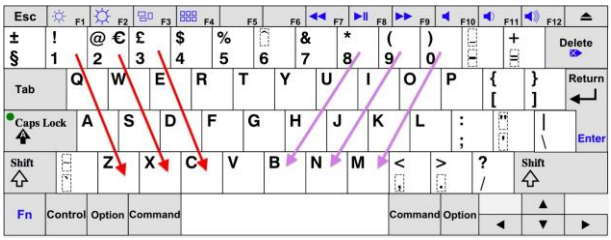

Figure- 4: Keys beneath number

5. *Change Keyboard*

Installing Unicode font, use this font with a passphrase, e.g., for PW "eastorwest" using the same keys on the keyboard, but with Kurdish Unicode it produces "ەاستوروەست". This technique enables selecting what could be remembered easily in any language and complex it by typing utilizing a different keyboard. Moreover, a user can mix between different keyboards, e.g., "eastorwestەاستوروەست".

C. *Substitution Techniques*

1. *Something from Cryptography*

At a minimum, you can set yourself up with a random but a straight substitution cipher (e.g., A→R, B→G, C→L, …etc.) to apply to the specific string, you can utilize keyboard to remember the substitution. Even this would not be hard to deduce if someone wanted to put a little more work into it, but it is a lot better than an immediately obvious tag like AMA or MBN. Moreover, it is practically simple, but ciphering should be kept safely.

2. *PW Encryption*

Cipher text in encryption is converting the readable data format to an unreadable format. Only the owner of cipher key can decipher the message into readable text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable [13]. Writing PWs in a file and encrypting the file and saving it in a cloud could protect PW [22]. In this way, if a hacker grasps encrypted text he cannot decrypt it because he does not know the private key. The security of this technique depends on maintaining the security of the private key.

3. *The Replacements*

Replacing certain characters with others is a great technique that is commonly used, but it is executed poorly. It is not that clever to replace character a's with @ or character o's with zeros because this is using LEED or 1337 language that is well known by hackers. Instead, use own replacement strategy by replacing some letter

with numbers, punctuation, or other letter (e.g., s→c, ch→k).

4. *USING CODES, TURN LETTERS INTO NUMBERS OR VICE VERSA*

First, consider an expression, and write that expression applying the numbers located on the phone number pad. The characters have now become digits. Adding an arbitrary character or symbol as well will raise the security of this PW. Replacing digits for characters is referred to as LEED or 1337 language. This method is programmed inside almost all PW cracking tools, can make it relatively less immune. Keep in mind to make this an element of a bigger PW or compound PW or use a personal substitution. For example "beStrong" convert to "835720|\|6" or "|33T2@|\|9".

5. *FOREIGN AND SLANG*

If a user knows a foreign language, he can throw some of those words in there, too. It is not necessary to create whole PW in a different language, but mix multiple languages to increase the entropy or the pool of possible words someone would have to test to crack a PW.

6. *ROUND WAY*

Exactly what makes a PW predictable is not simply the meaning of a PW, but likewise the real utilized words. One method to stop this problem is to declare something in an indirect way. For example, rather than making use of the PW "my sis", put it this way: "my mommy's other half's child" [2].

This pattern typically works well; simply beware not to use an easily guessable number such as a social security number or any commonly known number. Although, the pattern"(888) 888-eight eight" could seem repeated and easily, the fact that we utilize spaces, -, (), and that it is 22 characters long makes it a challenging PW to break [2].

D. Misilionces Techniques

1. *OVER PUNCTUATING*

Punctuation makes a PW memorable, and strongest: memorable because we are familiar with punctuation in normal writing and strongest because it increases entropy and length. Punctuation is the knife of PW mangling. Merely adding one punctuation symbol to all PWs will do wonders for PW security. The whole purpose of PW mangling is to ensure that someone cannot crack a PW based on a common word list. There are many word lists available, and some are quite effective.

All it takes to make sure a PW does not appear on a wordlist is adding a few punctuation symbols. There are many things one can do with punctuation, including delimiting, bracketing, prefixing, suffixing, pattern building, and so forth. Here are some examples: "After---->wards"," //lava//outlaw//", "Lenny-the-pirate"," Mister :) AOL", "hide the ***** PW", "--==//jetsons\\==--", ".....sleeping again...zzzz"

When using punctuation in a PW, do not forget about the special symbol characters. Also, remember that most modern operating systems consider the space to be a symbol character, so make good use of spaces as well.

2. *CONNECT THE FIRST LETTERS OF A PHRASE*

Establish a PW by using the very first letters of a sentence or phrase that indicates something - like a favorite football team or a historical hero. For example, "Don't purchase it, Argos it" would end up being "DpiAi.".

3. *CHOOSE WORDS AND COMBINE THEIR LETTERS*

Select one letter of the very first word and one letter of the second word, and repeating this until getting to the last letter of each word. An example can be residence & aircraft became PW= raeisricdreanfcte.

4. *MANGLING*

Mangling is changing, distorting, mutating, or deforming a common phrase into something unique. PWs that use diverse characters are strong and long, but diverse, long, and mangled PWs are the strongest.

Writing a phrase in a different dialect or accent is a great technique because the potential humor is easy to remember, and the modifications are easy to remember how to accurately reproduce, e.g., use accent to modify the phrase:

"I have fallen and I can't get up!" → "Redneck Ahve fallen an' ah can't gittup!" [2].

5. *RUSHING, SLICING, AND DICING*

Rushing is an extremely easy method; all thing need to do is mix things up a bit. Move words around, reverse the significance, or whatever it takes. Cutting and dicing resembles selecting a PW then taking a knife to it (e.g., near ly noon in norway).

E. Master Technique is Combining Multi Techniques

Combine several techniques make a PW strongest, combine numerous techniques that describe before create a truly remarkable yet extremely strong PW. Combine some techniques mention in this paper empower the security of PW. For example, combine replacement, repetition, punctuation, and shift button for PW "eastorwest" convert it to "eactEAST/or/wectWEST". The strength of a PW production system is not exactly how numerous letters, digits, and symbols wind up with, but exactly how numerous could get a various result utilizing the same system.

ANALYZING AND DISCUSSING OF THE SURVEY

In this paper, different ways are utilized to collect related information as indicated in section 3. The aim was analyzing and discussing currently using of PW. The

survey has been sent to more than one thousand users, 30% of them replay the survey. The academic levels of responders were 11% Ph.D. degree, 23% M.Sc. degree, 46% B.Sc. degree, and the rest were at a lower academic level (i.e., 20%). Based on the survey, approximately, all responders using PW, in our questionnaires 92% of responders have experience with PW for more than four years (8% less than four years experience). 25% used PW for more than ten programs. However, the high percentages of responders have not used PW powerfully, as indicated here: a third of them declare that they do not change their PW at all! Moreover, 20% used to write down their PWs to remember it. The reasons behind the bad utilization of PW refer to: they depend on memorizing PW; 77% of PW users who participate in our survey indicated that as shown in figure 5. Therefore, they build naïve and easy to remember. Also, PW 78% displayed zero information about all PW manager software. Due to these reasons 20% of responders were hacked.

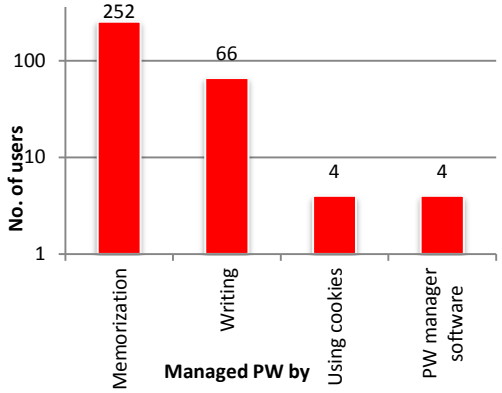

Figure- 5: Managing PW (Y-axis is on a logarithmic scale)

Moreover, the following percentages show mistakes of using PW:

- 34% used only letters and number for building their PW (i.e., 66% used letter, number, symbols, …etc.),
- 47% used same PW in ten accounts (i.e., 53% used different PW),
- 10% indicated having only one PW for everything (i.e., 90% having more than one PW),
- The average length of PW users were:
  - 15% of users were less than 7 characters,
  - 40% were 8-10 characters,
  - 30% were 10-15 characters,
  - Only 15% PW were lengthened more than 15 characters.

CONCLUSIONS

The PW has been used widely as a means of IS security (i.e., user authentication), but it includes some shortcoming. Researchers and developers should cooperate to make PW stronger and easer. Easy way to slightly increase the security of PWs and could be memorable as well, is personally design a PW generator techniques and combine several techniques. However, a user should pursue better PWs, not the best ones because the best tend to be unmemorable. IS user needs to take guidance from these methods as he comfy with and no more. This paper presented 24 techniques of easy to remember and hard to guess techniques. Utilizing these techniques, assists users building a strong PW. Therefore, bad utilization of PW, which indicated by the survey, could be improved because currently most users depend on building naïve and easy to remember PW.

BIBLIOGRAPHY

[1] 3 Ways to Create a Password You Can Remember - wikiHow: *http://www.wikihow.com/Create-a-Password-You-Can-Remember*. Accessed: 2014-04-29.

[2] Burnett, M. 2006. *Perfect password: Selection, protection, authentication*. Syngress Publishing, Inc.

[3] Carnavalet, X. de and Mannan, M. 2013. From very weak to very strong: Analyzing password-strength meters. *Network and Distributed System*. (2013).

[4] Charoen, D. 2014. Password Security. 8 (2014), 1–14.

[5] Chen, N. and Jiang, R. 2014. Security Analysis and Improvement of User Authentication Framework for Cloud Computing. *Journal of Networks*. 9, 1 (2014), 198–203.

[6] Cheng, B. et al. 2014. Corporate social responsibility and access to finance. *Strategic Management Journal*. 35, 1 (Jan. 2014), 1–23.

[7] Cheswick, W. 2013. Rethinking passwords. *Communications of the ACM*. (2013).

[8] Das, A. et al. 2014. The Tangled Web of Password Reuse. February (2014), 23–26.

[9] Florencio, D. and Herley, C. 2007. A large-scale study of web password habits. *International World Wide Web Conference Committee*. (2007).

[10] Herley, C. and Van Oorschot, P. 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy Magazine*. 10, 1 (Jan. 2012), 28–36.

[11] Jakobsson, M. and Akavipat, R. 2012. Rethinking passwords to adapt to constrained keyboards. *Proc. IEEE MoST*. (2012).

[12] Karthika, M. and Ravi, R. 2014. CCT: An Efficient and Affordable User Authentication Protocol Defiant

to Password Pinching and Reclaiming. *International Journal of Advance Research in Computer Science and Management Studies*. 2, 2 (2014), 304–310.

[13] Kumar, V. and Raheja, G.S.S. 2013. Cryptography. *International Journal of Computers & Technology*. 4, 1 (2013), 29–32.

[14] Olusegun, O. and Ithnin, N. 2013. People are the answer to security: Establishing a Sustainable Information Security Awareness Training (ISAT) program in organization. *International Journal of Computer Science and Information Security*. 11, 8 (2013).

[15] Password Requirements Quick Guide | IT Services: *http://itservices.stanford.edu/service/accounts/passwords/quickguide*. Accessed: 2014-04-29.

[16] Phetmak, N. et al. 2014. Travel Password: A Secure and Memorable Password Scheme. *Intelligent Information and Database Systems*, (2014).

[17] Qader, N.N. 2014. Privacy Preserving Against Untrusted Browser Origins and Personalized Powerful Password Management. *International Journal of Multidisciplinary and Current Research*. April (2014), 377–385.

[18] Qader, N.N. 2014. Strategic Framework Of Multilayer Checkpoint For Database. *International Journal of Computer Engineering and Applications*. V, III (2014), 53–60.

[19] Rajakumari, K. 2014. The Large-Scale Online Password Guessing Attacks Against with Revisiting Defenses. 20, 1 (2014), 29–33.

[20] Sekhar, V. and Sarvabhatla, M. 2014. A Robust Biometric-Based Three-factor Remote User Authentication Scheme. *arXiv preprint arXiv:1401.1318*. (2014), 2–3.

[21] Vijayan, V. 2014. A Review on Password Cracking Strategies. *IJRCCT*. (2014), 8–15.

[22] Yue, C. 2013. All Your Browser-saved Passwords Could Belong to Us: a Security Analysis and a Cloud-based New Design. (2013), 333–340.

[23] YUVARAJ, M. et al. 2014. Implementation of Password Guessing Resistant Protocol (PGRP) to Prevent Online Attacks. *International Journal of Computer Science and Mobile Computing*. 3, 2 (2014), 815–826.