International Journal of Multidisciplinary and Current Research

Research Article

ISSN: 2321-3124
Available at: http://ijmcr.com

Privacy Preserving Against Untrusted Browser Origins and Personalized Powerful Password Management

Nooruldeen Nasih Qader

Iraq\University of Sulaimani\ Computer Science Department

Accepted 10 April 2014, Available online 25 April 2014, **Vol.2** (**March/April 2014 issue**)

Abstract

Recent researches reveal the necessity of terminating the incorrect notion that password is dead and confirms that these believe has been hurtful. And suggest a campaign to emphases developing password (PW) use. Because of usability, PW security stills the most used methods in information security (IS), it is also, consider most challengers to researchers and needs more improving. In fact, authentication, on the web is dominated by PWs, mandating that users select solid PW. In this study, I indicated using, growing, and ongoing of PW, and the necessity of efficient PW management, especially with web browser based applications. Therefore, I analyzed some of common PW managers. PW managers can manage easily a bunch of unique, strong, and secure PW, which link users to the various websites. On the other hand, I collected nowadays data about practicing PW security. The data were analyzed and shown the necessity of improving and utilizing PW. As well as, I proposed categorize PW users, this categorization helps: IS developer to be more realistic when they design application and security polices, also, directs users to select appropriate strategies and techniques.

Keyword: *Security; Password; Phishing; hacker; usability; authentication; web; LastPass; KeePass*

1. Introduction

Recent researches indicate the necessity of ending, stopping and terminating the incorrect assumption that PassWord (PW) are dead and proves that this believe has been painful, discouraging research to find efficient ways to enhance the lot of approximately two billion people who utilize the PW. As well as shown that PW will stay with us in the future. And call for a campaign to emphases developing PW use. Substantial focus is applied coaxing PC users to choose good passwords, however, there is no concurrence about what power conditions need [1].

Web connected computers are definitely not secure at any place; many of the user PCs are affected with one or more forms of spyware or malware. Software application key loggers are installed on a user Personal Computer in addition to popular malware and spyware. A growing amount of phishing web sites likewise install key loggers on user computers, even when users do not clearly download or click any type of hyperlink on those sites [2].

Modern life communication with online resources is swiftly rising. Each website offers some capability, functionalities, and features to the user. These functionalities are special and occasionally important for the user. Functionalities vary from the fundamental emails (e.g., Gmail, Yahoo... etc) to some crucial transactional sites (banking, shopping... etc) [3], each stores information that is of importance to the individual. Some sites straight supply the details to the customer, while some particularly call for creating an account at that site to obtain the necessary specifics out of that web site. On the other hand, it is mandatory for safety needs to have distinct PWs for all such various web sites. With the expansion of the web solutions, a customer constantly develops brand-new accounts, each with a different user name and PW, bearing in mind is virtually difficult [4]. Analysis of using PW estimated many users choose PWs that are remarkably have low entropy [5], [6].

Computer users are asked to create, keep and remind an increasing number of PWs for host accounts, e-commerce sites, email servers and online financial services. Usually, PW authentication can resist brute force and dictionary attacks if users select strong PWs to provide sufficient entropy. The PW entropy that users can easily memorize seems inadequate to store unique and secure PWs for all these accounts. Thus, users reuse PWs across different websites [2]. PWs are a primary target of attackers for economically-motivated exploits, including those targeting online bank accounts and identity theft [7].

Authentication on the web is dominated by PWs, mandating that users choose strong PWs to achieve security. As the number of accounts each user is meant to support continues to grow, it is intractable for users maintain secure account management practices without aid.

PW authentication has common security and usability drawbacks. The researchers are continuing toward increasing the security and usability of PW authentication. Three-factor authentication is a complete defense mechanism in opposite to PW stealing attack, but it needs proportionally high cost and less friendly (e.g., users can easily forget or loss the token) [8]. Much more secure authentication methods have been proposed, due to the ease of deployment and usability issue; PWs continue to be the prime form of authentication of computer systems [2], [6]. In addition to traditional computers such desktops and laptops, people increasingly generating and using PWs with a wide variety of mobile terminals, such as tablets and Smartphones. Even with those PWs remain as the most convenient methods of authentication [9].

This paper is interesting in practical solutions combining easy deployability, security and usability [6]. The incumbency of PWs as the dominant authentication mechanism for the past several decades has created large psychological barriers to providing resistance to the adoption of radically different authentication technologies. Both users and service providers are most comfortable using PW authentication for reasons varying from culture to technology. An outright replacement of PWs will incur education and support costs that may be prohibitively expensive for small providers or free services.

On the other hand, PWs are most people's security weak points, annoying and they do not have the choice to deal with; but that does not have to be the case if we use a service to manage our PWs. E-commerce and secure web sites are not performing a hard work to protecting a personal data secure. 2013 saw a seemingly endless series of breaches that exposed PW data, at Adobe, Twitter, Tubmblr, and others. If the hacker discovers your PW, you are in difficulty. In case you have applied the same PW at other web pages, you are definitely in trouble. Internet users require to use a distinct and strong PW on each and every site, and the only realistic means to carry out that is with a PW manager [10]. PW manager encourages users to use stronger and more secure PWs, modern web browsers offer users PW management services. PW manager software retains much of the familiarity of PW authentication (e.g., usernames, PWs) [6].

Every user must enter their PW and username while logging into a session. Each of these sessions is prone to PW guessing attacks initiated by remote login systems or bot logins. Many login protocols have been implemented so far to resist such online PW guessing attacks [10].

The rest of this paper is organized as follows: literature survey is presented in the next section after that adopted techniques to gather required information about current practicing of PW has discussed. And then a major PW threats have displayed. Due to the role of PW building, the four roles of creating strong PW have presented. Common PW manager software has discussed. I proposed categorizing PW users, and then discussion and result. Finally, the conclusions of the study have exhibited.

2. Literature Survey

[11] Discussed incorrect assumption that PWs are dead has been hazarded, preventing research on effective ways to improve the bunch of around two billion consumers who use them. Every effort should be made to correct this. PWs have proven themselves a deserving opponent; all who have attempted to replace them en masse have failed. Usability of PW as well as innumerable attempts and near-universal passion to substitute PWs has been presented in [11], and shown that PW are more frequently used than ever before. The authors insist that, in many examples, PWs are the best-fit approach. Finally, the author displays the purpose of PW aging policies, realistic PW guidance, and PW managers improving.

[12] Presents the security analysis of two popular PW managers LastPass and RoboForm (both, browser and cloud based PW managers). The paper identifies several critical, high, and medium risk level vulnerabilities and provides some general suggestions to help improve the security of such tools.

The author of [13] proposes a new protocol Secure Session and PW Protection Protocol (SSPP) which asks for a machine name along with the Automated Turing Tests (ATT) approach for each login session. Then the user can detect whether there is an intrusion in between current and previous login, if the machine name changes. The SSPP keeps track of information about the user account and its activities with the help of some data storage lists. The primary aim of this protocol is to reduce inconvenience to legal users and prevent attackers from attempting remote logins.

[6] Proposes mechanisms of dual-factor authentication, involving possession of a Smartphone used in addition to a PW. They used Smartphone in authentication by generating a token (e.g., Google Authenticator) or to receive them (e.g., as one-time PWs over Short Message Service (SMS)). PWs are protected against offline attacks with a strong encryption key which the user need not remember, and decryption requires the control of two independent devices (e.g., a desktop PC and a Smartphone). It maintains security of the managed PWs by encrypting and storing the encrypted PWs on a Smartphone, keeping the decryption key inside the browser on the paired computer [6].

oPass provides users with a mechanism to authenticate from an un-trusted machine to an Internet service without revealing confidential user information which uses a user's cell phone and SMS to prevent PW stealing and PW reuse attacks [14].

[14] Studied backup authentication mechanism, they discussed and criticized adopting security questions and alternative email address.

Recently, mobile devices with touchscreens have made gesture-based authentication common. Tablets and Smartphones today are important for secure daily transactions. They are part of multi-factor authentication for enterprises. [15] Researches the security and safety and memorability of free-form multitouch gestures for cellular verification. This paper studies free-form multitouch gestures without visual reference; that is, gestures that allow all fingers draw a trajectory on a blank screen with no grid or other template.

With web services, a user always creates new accounts, each with a different user name and PW. [4] Proposes a new technique that uses two strong encryption algorithms, namely SHA256 and Two Fish algorithm to store the PW data.

3. 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 limited and specific use in information gathering. The benefit of a questionnaire is that it enables 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 huge quantities of data through questionnaires. In my questionnaires, I distributed the questionnaires to 1000 IS users and I receive the replay about 30% of them. After collecting questionnaires I review them thoroughly to make sure that the gathered information is valid. I use a questionnaire to obtain insight information about today practicing the use of PW. This information helps me to determine the areas that need further research, interviews, and observation. On the other hand, it discovers areas that need more improvement and techniques.
2. Conduct interviews and discussions with users. Interviewing is by far the most effective way to understand the limitations and obstacles. It is also, the most time-consuming and resource-expensive option. In this method, I meet PW users with different academic levels. A list of detailed questions is prepared and discussed. Obviously, this process may take some time, so it usually requires multiple sessions with each level. In order to conduct effective interviews, I organize this work in three areas: preparing for the interview, conducting the interview and following up the interview.
3. Observe and test, along with interviews, I conduct another useful method of gathering information that is observed and test directly multi PW user. As a result, I achieved wide experiences about using PW in information security. This first hand experience is invaluable to understanding exactly weak points in PW authentication processes.

4. Motivation Threats of PW Management

White Hat Security estimates that 83 percent of all the websites are vulnerable to at least one form of attack by the hackers. Generally, the stored files of a web application often contain information about the DBs the software needs to connect to. If the information in stored files is stored in plain text like many default installations do, it provides the keys for an attacker to get access to sensitive data [16], [17].

The biggest issue is some Information System (IS) cannot handle the requirements of security. One would ask about big enterprises (e.g., bank), how we trust today's IS security? Some of the common PW threats are described below:

4.1 Smart guesses

Many hackers simply try the most common PWs for a particular system. They might also try a blank PW and a PW that is the same as the username. If they get nothing, they just move on to the next account and keep trying until they find the accounts with weak PWs. If someone knows you, that person might try entering PWs related to your personal life- for instance, trying the name of your girlfriend or prized sports car. Someone might happen to know one or more PWs you have used elsewhere and try those. This technique is the most basic form of attack, but it is still very effective [18].

4.2 Dictionary attacks

Where all the possible keyword pair is formed as a dictionary and checked along with the guessed PW [10]. Dictionary attacks are typically offline attacks against a PW, but they may likewise be actually successful online when used correctly. Plenty of software tools are available to automate dictionary attacks against various systems. Most of these tools are effective enough to try out simple versions of dictionary words, for example, words subsequent by one or two numbers or basic character substitutions.

4.3 Brute-force attacks

Where checking every combination of all the possible PWs [10]. This type of attack could potentially take years to succeed, so it is often used as a last resort. Brute-force attacks are slow and time-consuming, but still quite common. These attacks are equivalent to trying every key on a huge key chain until you find the one that opens the lock. It is not uncommon for a hacker to obtain PWs for

50 percent of all hashes in just a matter of minutes.

4.4 Phishing

Phishing is a malicious activity whereby a phisher tries to trick the Internet users into providing confidential information. It is a serious problem because phishers can steal sensitive information, such as user's bank account details, social security numbers and credit card numbers by masquerading as a trustworthy entity in an electronic communication [2]. Sometimes a hacker can get your PW simply by asking for it. They might send you an e-mail claiming that your eBay or PayPal account is suspended, providing a place for you to enter your PW. The best defense for these types of attacks is simply never giving out your PW to anyone, no matter who you think they are [19]–[21].

4.5 PW reuse for multiple system

PW reuse is the reason for users to lose confidential information stored in various websites if a hacker compromises one of their PWs [2]. The strength of information system security varies from a system to another. We should avoid using same PW for the multiple account system. People have multiple accounts and they may reuse the same PWs for them, if hackers can gain access to one account, other accounts also cracked [7], [22]. For example, many users of email accounts have cracked because the users reuse the same PW for email system and Facebook account [23].

Computer users are asked to create, keep and remind an increasing number of PWs for host accounts, e-commerce sites, email servers and online financial services. Thus, currently, end users must remember too many PWs. The evolution of e-commerce has resulted in a massive increase in the number of PWs required by end users. The PW entropy that users can easily memorize seems inadequate to store secure and unique PWs for all these accounts causes users be likely to reuse PWs across different websites. [5] Reported that nearly everyone has only two or three PWs to access every account. Our questionnaires shown 57% of responders reuse the same PW for ten accounts, for more information refer to section 9. This can lead to the domino effect problem in which the hacker can gain access using one PW and then use the same PWs for other accounts [7]. Considering the huge number of PWs hacked and dumped on the Internet every day. Therefore, using same PW on multiple sites consider no longer a PW. Avoiding PW reuse is a crucial issue in information systems which can extend to PW stealing issue also [2].

PW reuse is the reason for users to lose confidential information stored in various websites if a hacker compromises one of their PWs. Many users of email accounts have cracked because the users reuse the same PW for email system and a Facebook account [23]. The PW entropy that users can easily memorize seems inadequate to store secure and unique PWs for all these accounts causes users be likely to reuse PWs across different websites.

4.6 Other techniques

Most login stores a valid cookie on the browser machine from which users had previously logged in successfully. Hackers can exploit vulnerabilities in Web browsers to obtain cookies that might contain authentication information [24]. They can use sniffers, specialized tools to watch network traffic to obtain PWs sent over the network unencrypted. They could even hold a gun to your head and just ask for your PW [18].

5. Strong PW Characteristics

You can run a quick test to make sure you are not choosing a common PW: Google for it. If you searched for your PW and nothing comes up, chances are your PW is sufficiently complex. Use basic rules as guidance in developing strong PWs as shown in figure 1. Follow these steps to increase your overall security and improve your PW Security:

1- The rule of complexity, eliminate weak PWs, Investigate and eliminate weak PWs. Makes a PW strong, ensures unpredictability and resistance to brute-force attacks. Our questionnaires shown 34% used only letters and number, and 15% of responders have PW length less than 7 characters, for more information refer to section 9.

2- The rule of uniqueness, every PW you use is exclusive to any particular system and distinct among all PWs. To avoid old PWs, refresh your PWs every three to six months. Here are some ways to make your PWs unique:

- Avoid PWs that include personal dates or other significant numbers, pet names, relatives or loved ones, vehicle names, favorite sports teams, or other personal information.
- Avoid getting too attached to a single PW.
- Avoid words or numbers relating to yourself or your environment.
- Avoid using common PWs, common phrases, or dictionary words.
- Never reuse the same PW more than once, especially among different systems. Reuse PW on multiple websites is extremely dangerous.

3- The rule of secrecy, stop storing PWs insecurely; if you are storing your PWs in your browser, on scrap pieces of paper, in an Email, in a Microsoft Word document, online in your Google Docs account, or in any format that is unencrypted, then you are taking a serious and unnecessary risk. Our questionnaires shown 20% of responders used to write down their PWs in order to remember it, for more information refer to section 9. Always maintain the secrecy and confidentiality of your PW to ensure its integrity as an authentication device. The following practices are necessary to maintain PW secrecy:

- Avoid saving PWs in Web browsers and other applications.
- Always delete e-mails that contain a PW.
- Use a Web site's logout feature rather than just closing your browser.
- Do not share your PW with others.
- Avoid recording your PWs in an insecure manner.
- Be smart with secret questions and answers.
- When the system is complete, use one PW while setting up and configuring a system and then change the PW.

4. Start using a multifactor authentication scheme, multi different elements that we utilize for authentication, something you know, something you have, and something you are. Using any one of these three methods is fallible, but combining two or more of them can have a huge impact on security. Using a multifactor authentication scheme significantly increases the security of confidential information.

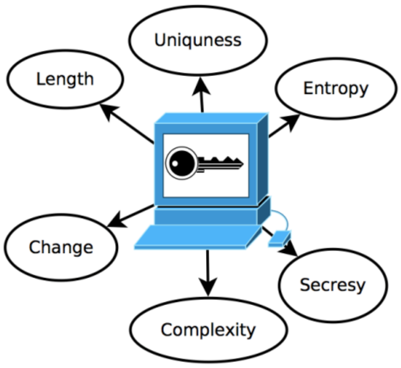


Fig.1 Required characteristics of strong PW

6. Web Browser Security

All browsers use Operating System (OS) PW as a key to encrypt PW; Mozilla Firefox is the only browser with a PW manager that operates identically across all OSs. If the master PW is set, then all stored credentials are encrypted using a triple-DES key derived from that PW [6], [25].

Web services (e.g., Gmail, Facebook, and online Banking) today most commonly rely on PWs to authenticate users. Web services often provide users with backup authentication mechanisms to help users regain access to their accounts. Current widely used backup authentication mechanisms such as security questions and alternate email addresses are unreliable or insecure or both [26].

7. Online Authentication and PW Manager

PW manager is an application that stores login information, PWs and user names, for Internet sites. Soon after these PWs are saved, the PW manager will authorize you to automatically fill in the username/PW fields on internet sites you visit, eliminating the requirement for you to minding your PW for every of your records.

Fairly a few PW managers let individuals log in to your PW repository from any web browser, so users may search for credentials even when utilizing someone else's personal computer. Among these are RoboForm Everywhere 7, Norton Identity Safe, and Keeper 5.0; Dashlane and LastPass also offer this attribute. F-Secure, by contrast, does not enable any on-line access gain, considering it is a possible security hazard.

KeePass is an interesting tool for PW management. Even though you still need to memorize the PW for the machine running this software, and the PW that opens the KeePass database, two PWs to bear in mind is a good compromise [10]

In practice, as with generative PW managers, retrieval PW managers require the customer only recall the master PW in order to confirm with all of the accounts enrolled in the manager. PW managers offer phishing protection by preventing PW entry at the faulty addresses [6].

The advantage of the system is that even if in mere future the customer takes place to forget the login of a website that has been accessed a long time back, it can be simply retrieved by the account working with the typical login ID details for the website. This website will set the customer free by making him remember just a single login ID and PW which in turn will retrieve the required login ID and its PW.

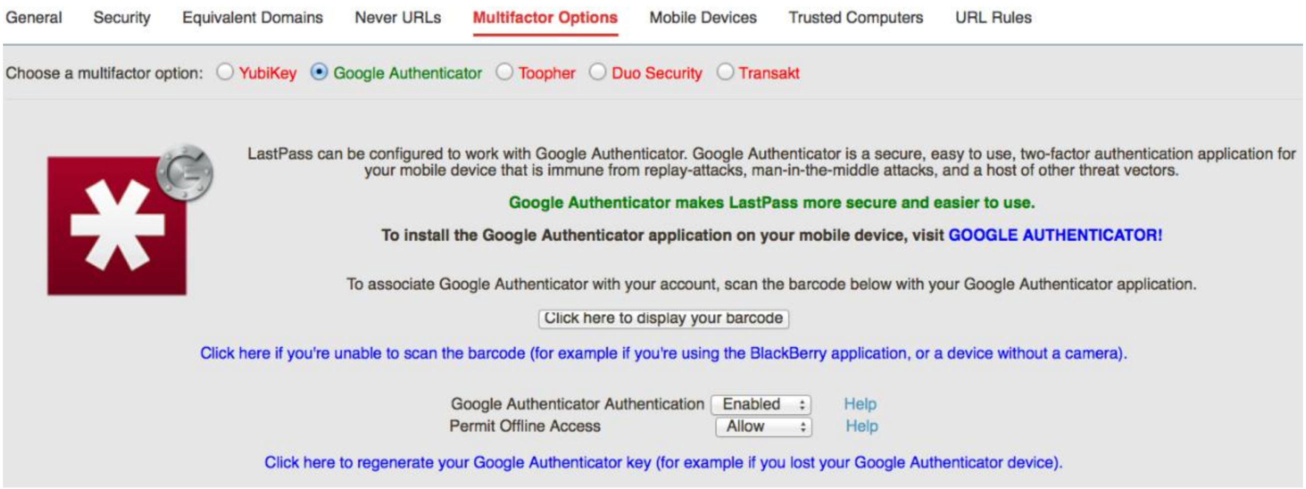
A number of retrieval PW managers are implemented as browser extensions [6] Numerous PW managers extend their service to Android and iOS devices, among them Dashlane 2.0, Norton Identity Safe, and Trend Micro DirectPass.

With so much bigger the Internet site coming to be targets of universal account unload, it is currently crucial than ever before that you never reuse the exact PW at any place. PW manager applications, build the process of developing, handling, and inputting PWs so easy; there may be no explanation to not utilize these products. If the system enables anyone, PWs are more vulnerable to attack than at any time; anyone should absolutely not generate a PW less than 15 characters but work with 20 or more. Handling this many strong, unique PWs is almost impossible to do at this moment without the help of a PW manager [10].

PW managers are designed to relieve PW fatigue, reduce cognitive load on accounts, and reduce login time. They may similarly indirectly facilitate better PW quality and a reduction in PW reuse. PW managers may also integrate other techniques to strengthen or encode PWs (e.g., biometric).

7.1 Levels beyond simple security

In case any individual is worried that a hardware keylogger may catch your LastPass master PW, anyone can enter it using the embedded virtual computer



Choose a multifactor option: ○ YubiKey ● Google Authenticator ○ Toopher ○ Duo Security ○ Transakt

LastPass can be configured to work with Google Authenticator. Google Authenticator is a secure, easy to use, two-factor authentication application for your mobile device that is immune from replay-attacks, man-in-the-middle attacks, and a host of other threat vectors.

Google Authenticator makes LastPass more secure and easier to use.

To install the Google Authenticator application on your mobile device, visit GOOGLE AUTHENTICATOR!

To associate Google Authenticator with your account, scan the barcode below with your Google Authenticator application.

Click here if you're unable to scan the barcode (for example if you're using the BlackBerry application, or a device without a camera).

Google Authenticator Authentication: Enabled — Help
Permit Offline Access: Allow — Help

Click here to regenerate your Google Authenticator key (for example if you lost your Google Authenticator device).

Fig. 2 LastPass PW manager multifactor options

keyboard. It does not matter if a keylogger captures one of these, or if an eagle-eyed spy shoulder-surfs your PW. Logging in will demand the two your master PW and a one-time code sent to smart phone if you link Google Authenticator to your LastPass account as shown in figure 2. LastPass even consists of a totally low-tech authentication method they call Grid Multifactor. After you log in with your master PW, LastPass will ask for the characters at specific intersections.

7.2 Security challenge

The major area of working with a PW manager is that it enables anyone halt using dumb PWs such as "PW" and likewise halt working with the exact PW on various web sites. As individuals add new sites, e.g., LastPass helps you generate new, strong PWs. With respect to the occurring weak PWs, several PW managers assess the power and replication of saved PW, and then advice the user to enhance poor PW.

For added security, anyone may restrict your LastPass profile to work only in specified countries, as well as set it to prohibit logging throughout Tor networks. You can easily set it to systematically turn off soon after a certain amount of idle time, to warn if anyone fills forms of non-HTTPS websites, and even more [10].

7.3 secondary attributes of PW managers

PW managers frequently perform a variety of auxiliary attributes and above the effortless management of PWs.
1- Backups, producing a backup that may be cached offline, and later employed for import back into the PW manager. If the backup is to stay secure, it must be encrypted.
2- Synchronization, it is allowing authentication with stored credentials from any one of the devices a user repeatedly utilizes in their consistent web site browsing, not only one primary machine where the manager initially installed.
3- Arbitrary PW production, some PW manager addresses a common weakness with retrieval PW managers by providing features available to develop the PW security features (high-entropy). Typically this is implemented in a way that authorizes the customer to select parameters controlling the PW generation that include length and the character classes (e.g., letters, numbers, symbols) utilized during generation [6].
4- PW quality inspection, in a similar vein, some PW manager pro-actively observes the PWs used by the customer in order to measure PW quality. Potentially weak PWs are flagged and the client may be notified that these PWs should be replaced/strengthened. LastPass additionally monitors for PW reuse, and notifying the client when the identical PW is detected as being used across more than one website/account [6].
5- Untrusted login, untrusted computers pose a problem for PW entry in general, but in particular for many access PW managers, as keyboard logging malware can simply access to the master PW. Several managers offer a means whereby clients can authenticate with the PW manager without disclosing their master PW (e.g., one-time PWs and virtual keyboard) [6].

Soon after these PWs are cached, the PW manager will authorize individuals to automatically fill in the username/PW fields on Internet sites, individuals explore, eliminating the demand for anyone to bear in mind your PW for any of your records. In practice, like with generative PW managers, access PW managers demand the end user basically remember the master PW in order to validate with all of the profiles enrolled in the manager. The primary area of using a PW manager is that it lets individuals stop employing stupid PWs just like "PW" and similarly stop employing the same PW on various Internet sites. Regarding the current weak PWs, several PW managers investigate the force and replication of saved PW, and then train the customer to improve weak PW.

7.4 The best PW managers

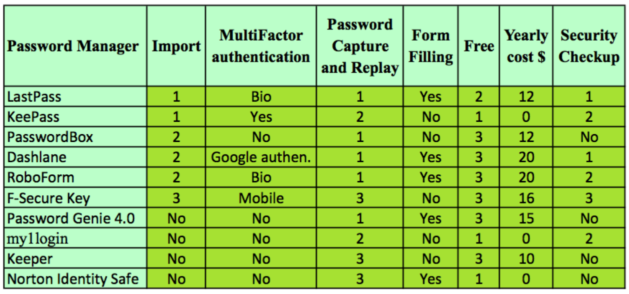
Table 1 shows an evaluation of some common PW managers. To indicate the meaning of numeric and ranking in the table 1, I describe *Security Checkup* feature. Virtually every PW manager may state the power of the master PW. Norton, RoboForm, KeePass, and quite a few some other can also rate each of your saved PWs. And virtually almost every product or services may create solid, arbitrary PWs for you on demand. LastPass and Dashlane make this idea a step more than. Each supplies a security document detailing each of your PWs plus ranking the strength of each. They also report on duplicates PWs you have used on over one site. As well as they make it easy to upgrade all your PWs to improve security.

After analyzing features of PW manager I prefer LastPass and then Dashlane, but each user should find one that best suits their needs. To know the personal impact on any PW manager test usability, flexibility, and security. Empirically evaluate the viability of PW managers, make sure you feel comfortable using the application; otherwise, you won't use it. There are alternatives to these tools that might work better in some situations. One may prefer more flexibility, security or balance between them.

Although of relative maturity and all those benefits of using PW managers, our questionnaires shown 78% of responders zero information about all PW manager software, for more information refer to section 9.

In general the rewards of utilizing PW manager may be listed as follows: reduces the bot logins from remote access, minimizes the disruption created by entering username and PW for acceptable users, guards the session information, and tracks down any effort of illegitimate access.

Table 1 Evaluation of popular PW manager software



Password Manager	Import	MultiFactor authentication	Password Capture and Replay	Form Filling	Free	Yearly cost $	Security Checkup
LastPass	1	Bio	1	Yes	2	12	1
KeePass	1	Yes	2	No	1	0	2
PasswordBox	2	No	1	No	3	12	No
Dashlane	2	Google authen.	1	Yes	3	20	1
RoboForm	2	Bio	1	Yes	3	20	2
F-Secure Key	3	Mobile	3	No	3	16	3
Password Genie 4.0	No	No	1	Yes	3	15	No
my1login	No	No	2	No	1	0	2
Keeper	No	No	3	No	3	10	No
Norton Identity Safe	No	No	3	Yes	1	0	No

8. PW User Category

The periods advocated using long, and unforgettable PW has gone. Nowadays the ideology has replaced toward using a PW manager and producing long, random PWs for each online account. At the same time I continue to use my personal easy-to-remember PWs for the Internet sites where I frequently should enter PWs manually, the mass of the PWs I generate now are long, random PWs that LastPass generates for me. Maybe even five years earlier (2007) it was feasible to manage and memorize ten or twenty unique PWs, but the world has replaced and it is not unusual for a common web individual to have dozens or even lots of internet accounts [10].

One may argue, if we have trusted and powerful PW manager software, we may no longer need to learn how to build a PW and easy to remember techniques. This logic is incorrect because:

1- In addition, of the web, we need PW to login to different OSs, Networks, hardware (e.g., Smartphone), and applications.

2- Most PW manager needs a master PW that should have efficient characteristics of PW because the entire security of PW manager depends on this PW. Moreover, most of PW managers offer features to generate PW based on, which in turn need awareness and realization of powerful PW.

3- Trustiness is a relative issue, as there are classes of users trust easy, also, there are classes of people that does not trust any PW software manager.

Therefore, we should know how to build PW and improve the characteristics of PW.

Even for web services there are levels of security regarding PW. Some websites which have a constraint of compulsory registration before accessing the contents of the website. Some confidential data (e.g., credit card numbers, account numbers… etc.) is of crucial importance to the user. There lies one more level below, which stores, the less critical information (e.g., The user's mailbox PWs, drop box PW, free messaging websites PWs… etc.) [4], [22]. Now days, many websites have a 'Login with Facebook' facility provided for registration. However, this facility is available only for less critical and tolerant websites. The aim of these features work is to provide the user with a direct login facility [4].

Storing many PWs all in one location could pose a security threat, offering an attractive target for an adversary. To alleviate these concerns, many retrieval PW managers rely on a master PW that must be provided to unlock (by means of decryption) the stored PWs [10].

Three-factor authentication is a complete defense mechanism in opposition to PW stealing attack, but it needs proportionally high cost [2].

Figure 3 shown PW categories. IS users dealing with PW, but in different classes, classes differ from multi perspective:

1. Quantity, while some people have few places that need PW, there are other peoples having dozen places and the list of those places is rapidly growing. PW memorization is possible with few places, but with dozen places we need to find a suitable PW manager.

2. Security level, for crucial data user worry about issues such as: How does store the data, and where? Is it encrypted well enough? Can I trust the people and cloud-based application? Especially if you use an online service you are giving your whole digital life into the hands of some tools that may or may not be secure enough to store your PWs. As a programmer, you might be able to verify that e.g. KeePass is working and encrypting good

enough, but what should the *general people* do that cannot even know how some online service works [10].

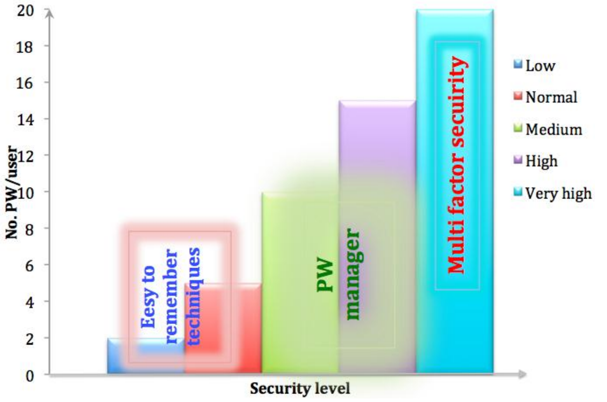


Fig. 3 PW users categories and appropriate security strategy

For a specific application, how many security layers should be used? Which layers and mechanisms? How it is configured? All these answers depend on the value of information that must be secure, the nature of the attacker, are the storage environment changed from time to time, and moved from place to place, or in general from environment to other [23].

3. Confidence and trusty, as I said earlier trustiness is a relative issue, as there are classes of users trust easy, also, there are classes of people that does not trust any PW software manager (they focus on the case where an attacker may crack the administrator account for the web server). Therefore, PW manager follows different ways to gain users' confidence. For example, KeePass offer combination of master PW and key file to open a user account [10]. If storing encrypted PWs in the cloud or even on the PC makes you nervous. The best PW manager is MyLOK Personal; it stores your PWs and personal information in a smart card encrypted by an on-board crypto chip. No Internet hacker can get access to your PWs when they are stored in encrypted EEPROM in a USB device in your pocket. However, competing PW management solutions offer more features and more flexibility [10].

9. Discussion and Results

In this paper, different ways are utilized to collect related information as indicated in section 3. The study utilized multiple data sourcing method: personal observation, oral interview, focus group discussion, and questionnaires. The aim was analyzing and discussing the nowadays practicing of PW. The survey has been sent to one thousand of IS users, I received the responses from 303 users. The academic levels of responders were 11% PhD degree, 23% M.Sc. degree, 46% B.Sc. degree, and the rest were lower academic level. According to the survey, almost all computer users dealing with PW, in our questionnaires 92% of responders have experience with PW for more than 4 years and 25% used PW for more than 10 programs. However, high percentage of responders not used PW powerfully, as indicated here: 34% used only letters and number for building their PW as shown in figure 4, 47% used same PW in ten accounts, furthermore, 10% indicated having only one PW for everything, and the average length of PW for each users were 15% less than 7 characters, 40% were 8-10 characters, and 30% were 10-15 characters, only 15% PW were lengthened more than 15 characters as shown in figure 5.

Moreover, 30% states that they do not change their PW at all! And 20% used to write down their PWs in order to remember it. The reasons behind bad utilization of PW refer to: they depend on memorizing PW; 77% of PW users who participate in our survey indicated that. Therefore, they build naïve and easy to remember. Also, PW 78% displayed zero information about all PW manager software. Due to reasons 20% of responders were hacked.

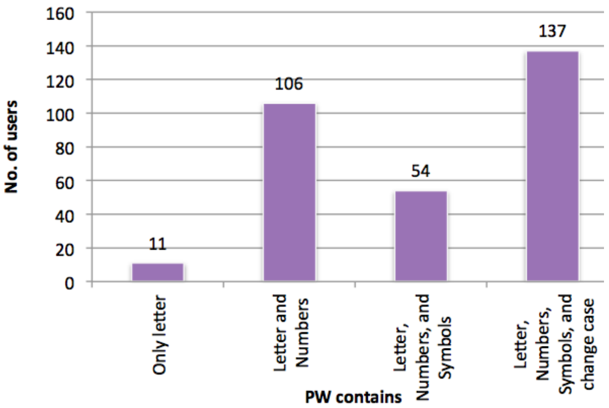


Fig. 4 Number of users and PW contain

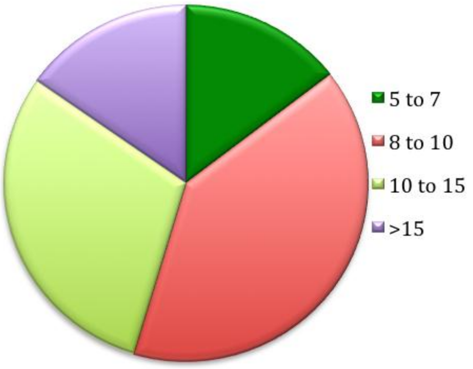


Fig. 5 Average PW length

10. Conclusions and Future Work

Due to usability advantage, PW security stills the most used methods in IS, it is also, consider most challengers to researchers and needs more improving. In fact, authentication, on the web is dominated by PWs, mandating that users select solid PWs (most often manually) to achieve security. Therefore, one of the primary goals of researchers is to reduce inconvenience to legal users and prevent attackers from logins by maintaining PW authentication. In this study, I indicated continuous, growing, and using of PW, and the need of efficient PW management, especially with web browser based applications. Therefore, I discussed some of common PW managers. PW managers can manage easily a bunch of unique, strong, and secure PW, which link users to the various websites. Security of most common PW managers depends on master PW. Thus, master PW needs to be replaced at frequent periods [4].

On the other hand, I collected today's data about practicing PW security. The data were analyzed and shown the necessity of improving and utilization of PW. Therefore, in the next work, I propose more techniques of building strong and remembered PWs. As well as, I proposed categorize PW users upon: quantity, security level, and confidence. This categorization helps: IS developer to be more realistic when they design application and security polices, also, directs users to select appropriate strategies and techniques. There are many existing techniques that concentrate on a particular challenge and may be convenient for a particular group of user, but they certainly need more reinforcement.

References

[1] C. Herley and P. Van Oorschot, "A research agenda acknowledging the persistence of passwords," *Secur. Privacy, IEEE*, 2012.

[2] S. Aghav and R. Bedi, "Authentication Mechanism for Resistance to Password Stealing and Reuse Attack," *arXiv Prepr. arXiv1402.6497*, 2014.

[3] S. M. Pourkiaei, S. Sadat, and V. Ardestani, "Internet-Banking: A Way of Life," *Intational J. Multidiscip. Curr. Res.*, vol. 2, no. April, pp. 226–229, 2014.

[4] D. Ingle, V. Patil, and S. Talbar, "Password-Free Login.," *Int. J. Comput. Appl.*, vol. 87, no. 17, pp. 26–30, 2014.

[5] Y. Yang, J. Lindqvist, and A. Oulasvirta, "Text Entry Method Affects Password Security," *arXiv Prepr. arXiv1403.1910*, 2014.

[6] D. McCarney, "Password managers: comparative evaluation, design, implementation and empirical analysis," CARLETON UNIVERSITY, 2013.

[7] N. Qader and L. Geroge, *Design and Implement a Secure Database Using Multi Level Security*, Holsen. LAP LAMBERT ACADEMIC, 2014, p. 125.

[8] V. Sekhar and M. Sarvabhatla, "A Robust Biometric-Based Three-factor Remote User Authentication Scheme," *arXiv Prepr. arXiv1401.1318*, pp. 2–3, 2014.

[9] D. Charoen, "Password Security," no. 8, pp. 1–14, 2014.

[10] "My Advice: Just use a Password Manager | Xato - Passwords & Security," 2014. [Online]. Available: https://xato.net/passwords/use-a-password-manager/#.Uy58P14aZas. [Accessed: 23-Mar-2014].

[11] C. Herley and P. Van Oorschot, "A Research Agenda Acknowledging the Persistence of Passwords," *IEEE Secur. Priv. Mag.*, vol. 10, no. 1, pp. 28–36, Jan. 2012.

[12] R. Zhao and C. Springs, "Vulnerability and Risk Analysis of Two Commercial Browser and Cloud Based Password Managers," 2013.

[13] M. Resmipriya and M. G. M. Sangeetha, "An Efficient Approach for Preventing Online Password Guessing Attacks," vol. 2, no. 3, pp. 1959–1962, 2013.

[14] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 651–663, Apr. 2012.

[15] M. Sherman, G. Clark, and Y. Yang, "User-Generated Free-Form Gestures for Authentication: Security and Memorability," *arXiv Prepr. arXiv …*, 2014.

[16] S. Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions," *Intational J. Multidiscip. Curr. Res.*, vol. 2, pp. 62–69, 2014.

[17] G. M. J, "Database Security: Best Practices for Securing The Database Of A Small Businesses," vol. 2, no. 7, pp. 1–4, 2013.

[18] M. Burnett, *Perfect password: Selection, protection, authentication*. Syngress Publishing, Inc., 2006, p. 200.

[19] A. A. Khan, "Preventing Phishing Attacks using One Time Password and User Machine Identification," vol. 68, no. 3, pp. 7–11, 2013.

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

[21] E. Grosse and M. U. Google, "Authentication at Scale," no. February, 2013.

[22] O. Olusegun and N. Ithnin, "People are the answer to security: Establishing a Sustainable Information Security Awareness Training (ISAT) program in organization," *Int. J. Comput. Sci. Inf. Secur.*, vol. 11, no. 8, 2013.

[23] N. N. Qader, "Implementing I & A in Multilayer Checkpoints for DB Security," vol. 5, no. 2, pp. 4–14, 2014.

[24] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *2012 IEEE Symp. Secur. Priv.*, vol. 2012, pp. 553–567, May 2012.

[25] K. Bhargavan, "Language-based Defenses against Untrusted Browser Origins," *Proc. 22nd USENIX Secur. Symp.*, pp. 653–661, 2013.

[26] N. Gong and D. Wang, "On the Security of Trustee-based Social Authentications," *arXiv Prepr. arXiv1402.2699*, 2014.