An Assessment of Website User Authentication Mechanisms
Samia R.Madhusudhan and Chaitanya S. Nayak
Pages 14 – 20
DOI: http://dx.doi.org/10.21700/ijcis.2018.xxx

An Assessment of Website User Authentication Mechanisms

R.Madhusudhan[1] Chaitanya S. Nayak[2]
Department of Mathematical & Computational Sciences,
National Institute of Technology Karnataka, Surathkal, Karnataka, India
madhu_nitks@yahoo.com[1] chaitanyasnayak19@gmail.com[2]

Abstract*:* Even after decades of internet evolution, passwords still remain the dominant means of user authentication. With an increasing range of websites, which store and allow access to sensitive personal information, the way in which users are authenticated to online services is going to be an important consideration in order to prevent problems like unauthorized access and information theft. This paper presents a survey on password practices of nearly 36 websites, discusses the weak areas in present practices regarding the choice of passwords of users and various security questions in case the user forgets password, and gives guidelines for improvement.

Keywords: *Passwords, Authentication, Awareness, Guidelines, Websites, Restrictions*.

Received: *July 30, 2016* | **Revised**: *August 10, 2016* | **Accepted**: *Janaury 25, 2017*

1. Introduction

The Internet is a gift of modern science that has created a revolution around the globe in almost every field. All the activities of human life have been touched by the Internet in one way or the other. So we see a vast growth in usage of online services [1] which includes online banking, online shopping, social networking etc. When the public is relying so much on web services, hackers are busy challenging the security of such services and secret information. So, network security is one of the major concerns for experts working in the area of computer networks. However, majority of our online accounts are protected by the traditional combination of username (or email address) and password [9]. But users make it vulnerable because of their bad password practices, mostly due to lack of awareness. A lot of surveys were made to find the most common weak passwords [8, 11, 12]. A survey on popular password choices reveals that the most common ones are among the worst imaginable – e.g., the top five [8] are: password, 123456, 12345678, abc123 and qwerty. This suggests that many users still have significant lessons to learn in terms of how to choose passwords effectively making them more secure as well as more difficult for adversary to crack them. Also, they are ignorant about the threats they might have to face during accessing online services due to weak passwords. Choosing such passwords may be either because users will be aware of the challenges but difficult to memorize complicated passwords or they have zero knowledge about possible danger they are in due to weak passwords. So, it becomes necessary for security departments to guide users regarding security issues and password selection. This is possible only when there is clear communication between security departments and the users.

Most of the websites monitor the password and show status of the password like weak, medium or strong. Unfortunately, many of them do not restrict the password to follow the security guidelines. Many sites (like e-commerce sites in our survey) do not restrict the pattern of password. Upon that, even the restriction on length of passwords is considerably low. The leakage of passwords from three major websites has highlighted the dangers of poor password protection practices. LinkedIn, eHarmony and Last.fm all suffered breaches within a few days [10].

We made a survey on password practices including the password type, ways of retrieval of passwords and the restrictions on passwords of 36 different websites. Besides the bad practices of users, we found that there are many websites, which does not restrict the users to choose secure passwords and does not give guidelines for choosing a strong password.

The rest of this paper is organized as follows. Section 2 contains security questions used for identifying legitimate user, section 3 relates user-friendliness and security, section 4 discusses the survey result, and section 5 gives guidelines for choosing passwords followed by conclusion in section 6.

2. Security Questions Used For Identifying Legitimate User [3, 19]

It often happens that user forgets the password due to various reasons. In such situations, the websites should help the user in retrieval of password and/or provide options for the user to choose a new password; making sure that only the legal user is provided with such an option. Usually, this is done through registered email or with the help of users' mobile number or by asking the so-called security questions. Most of the websites go for security questions. If the user enters the correct answers (which are initially saved by the user during registration), it means he/she is the legal user and is eligible to choose a new password. But, it is not necessary that only the legal user must produce correct answers. Most of the times, the questions will be in such a manner that a close friend or spouse can guess the answers correctly with less or no effort. This raises a question as to whether such questions can really be called as secure questions! Unfortunately, the answer is no. The common security questions that eBay, yahoo, etc., use are stated below:

- What street did you grow up on?
- What is your mother's maiden name?
- What is the name of your first school?
- What is your pet's name?
- What is your father's middle name?
- What is your mother's birthplace?
- What is your grandfather's occupation?
- What is the name of your favorite teacher?
- Who is your best childhood friend?
- What is your school's mascot?
- Who was your childhood hero?
- What is your favorite pastime?
- What is your all-time favorite sports team?
- What was your first car or bike?
- Who is your favorite cricketer/sportsperson?
- Where did you first meet your spouse?
- What is your date of birth?
- When was your first child born?

Some websites use these type of security questions in password retrieval phase. The first seven questions can be answered by family members whereas friends knew the details about favorite car or bike or sports team and questions at the end can be easily answered by spouse as well. Then where comes the security when people other than the legitimate user can answer the questions accurately? How secret are in fact the 'secret questions' used for resetting forgotten passwords? According to a published study [20], 17% of its participants were able to answer the 'secret questions' of strangers and also indicated that the most popular questions were in fact the easiest ones to answer.

The best practice of choosing the question is to choose the question in such a way that the answer should not relate to public information and should not be answered by spouse/close friends etc. Also the question should be framed in such a way that there should not be any ambiguity for the user to answer.

3. User friendly Versus Security

Simple passwords which are user friendly (easily remembered by the user) are not secure and can be cracked by some hacking tools like Ophcrack [4, 5] and using social engineering methods. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed [6]. Although the best practice of choosing the password is a pattern mix of alphabets, numbers, special characters, capital letters and small letters, it becomes user unfriendly. If humans didn't have to remember their passwords, a maximally secure password would have maximum entropy [16].

The common pitfalls [2, 14, 17] that make passwords vulnerable are:

- Weak password choices (short, based on dictionary words, common passwords like 1234, etc.).
- Using the same password on multiple systems, which makes it easy to break into all the systems on compromising any single system.
- Retaining the same password for longer periods.
- Writing or storing the information of passwords.
- Accessing the online accounts on public systems where there can be risk of tracking or monitoring the usage.

For creating a complex password and at the same time to easily remember it, user can use some techniques that will help him remember the password. For example, using first letters of the phrase "The entire world is termed as a global village recently", we can make "Tewitaagvr" as a

password. To make it more complex, the user simply needs to add some of his favorite characters or numbers in between the letters. Users have to be treated as partners in the endeavor to secure an organization's systems, not as the enemy within. System security is one of the last areas in IT in which user-centered design and user training are not regarded as essential—this has to change [6]. Equal participation of security departments and users can result in more secure mechanisms which is very much necessary in the present scenario.

4. Survey Result

We have done a survey on different websites, which includes different types like social networking, e-commerce, online banking, mail service, etc., and the results are shown in Table 1 and Table 2, We have considered issues like the type of the password accepted, whether it is mandatory or not, option of user to choose his own user id, whether the initial password is given by the server or the user chooses his own password. These results are shown in Table 1. We have also made a survey on the password retrieval methods (if password is lost) of various websites and restrictions in choosing the password. The results are shown in Table 2.

From the Table 1, it is evident that almost all the banking sites does allow user to choose his/her own username but password is sent in a different manner other than the rest of the websites. Almost all the e-commerce websites make use of the registered email as his/her user id and ask to choose a password in the registration process.

Table 1− Comparison of websites based on password type and its requisiteness, choice of user ID and initial password.

Name of the website	Password Type Mandatory	User Chooses UID	Initial Password Given By Server?	Name of the website	Password Type Mandatory	User Chooses UID	Initial Password Given By Server?
onlinesbi.com	Yes	Yes	Yes, through post	flipkart.com	No	No-Reg Email	No
yahoomail.com	Yes	Yes	No	snapdeal.com	No	No-Reg Email	No
kvb.co.in (bank site)	Yes	No	Yes, through Registered mail	yebhi.com	No	No-Reg Email	No
bsnl.co.in	Yes	Yes	No	myntra.com	No	No-Reg Email	No
ksrtc.in	No	No-Reg Email	Yes	futurebazaar.com	No	No-Reg Email	No
apsrtconline.in	No	Yes	Yes	way2sms.com	No	No-Reg Phone	Yes
ebay.in/.com	Yes	Yes	No	160by2.com	No	No-Reg Phone	Yes
corpretail.com	Yes	Yes	Yes, through post	stayzilla.com	No	No	No
irctc.co.in	No	Yes	No	lensbazaar.com	No	No-Reg Email	No
gmail.com	No	Yes	No	jabong.com	No	No-Reg Email	No
facebook.com	No	Yes	No	shopperstop.com	No	No-Reg Email	No
skype.com	No	Yes	No	coursera.org	No	No-Reg Email	No
amazon.com	No	No-Reg Email	No	zurker.com	No	No-Reg Email	No

tradus.com	No	Yes	No	indyarocks.com	No	Yes	Yes
healthkart.com	No	No-Reg Email	No	indiaplaza.com	No	Yes	No
lenskart.com	No	No-Reg Email	No	homeshop18.com	No	No-Reg Email	No
dropbox.com	No	No-Reg Email	No	shopclues.com	No	No-Reg Email	No
karnatakaholidays.net	No	No-Reg Email	Yes	infibeam.com	No	No-Reg Email	No

But some websites like ticket booking sites are sending initial password to the registered mail or mobile number and later they allow the user to change the initial password. Almost all the websites offers sms service to send the initial password to the mobile for the sake of verification of mobile number. This suggests that most of the sites let the user choose the password without imposing any conditions or rules.

From the list of websites in the table 2, onlinesbi.com, ebay.com, corpretail.com, kvb.co.in and bsnl.co.in restrict the users to follow patterns of mixing alpha numeric symbols. Almost all the websites have restrictions for password length except infibeam.com among the list of websites in Table 1 and Table 2. The websites that offer

Table 2 − Comparison of websites based on retrieval methods of password and restrictions on choosing password

Name of the website	Retrieval if password lost	Restrictions on choosing password
onlinesbi.com	Using profile password; if profile password lost, then through post/ branch	Mix of alphanumeric symbols, 8 to 20 characters required
yahoomail.com	Reset through phone	Mix of alphanumeric, one capital letter, one small letter compulsory,8-32 characters
kvb.co.in (bank site)	Through registered email	Mix of alphanumeric, one capital letter, one small letter
bsnl.co.in	Through registered email/phone	Minimum 8 characters, must be mix of alpha numeric characters
ksrtc.in	Through registered email	6 to 15 characters required
apsrtconline.in	Through phone	Mix of alphanumeric symbols , special characters
ebay.in/.com	Through registered email	Mix of alphanumeric symbols
corpretail.com	Through registered mail/mobile after answering security questions	Mix of alpha numeric symbols
irctc.co.in	Through registered email after asking security questions	4 to 10 characters required
gmail.com	Reset through phone/alternate email	Minimum 8 characters required
facebook.com	Through registered email/phone as users wish	Minimum 6 characters required
skype.com	Through registered email	Minimum 6 characters required
amazon.com	Through registered email	Minimum 6 characters required

tradus.com	Through registered email	Minimum 6 characters required
healthkart.com	Through registered email	Minimum 6 characters required
lenskart.com	Through registered email	Minimum 6 characters required
dropbox.com	Through registered email	Minimum 6 characters required
karnatakaholidays.net	Through registered email	Minimum 4 characters required
flipkart.com	Through registered email	Minimum 4 characters required
snapdeal.com	Through registered email	Minimum 4 characters required
futurebazaar.com	Through registered email	Minimum 4 characters required
way2sms.com	Through phone	Minimum 4 characters required
160by2.com	Through phone	Minimum 4 characters required
stayzilla.com	Through registered email	Minimum 4 characters required
lensbazaar.com	Through registered email	Minimum 4 characters required
jabong.com	Through registered email	Minimum 4 characters required

sms service sends the new password or the old password to the registered mobile number. When it comes to password retrieval phase, most of the websites system of password retrieval is through registered email. Some popular websites like irctc, Facebook and eBay ask for security questions during password retrieval phase to authenticate the user.

By observing the survey results, it is clear that the websites that offer banking services are taking maximum care in matters of restrictions. Unlike many other websites, Facebook restricts its users from reusing any of their old passwords. Many systems and sites tend to advise and prescribe what should be done without really explaining why [9]. Hence, the user fails to understand the need for a strong password.

5. Guidelines for choosing the password

It is common tendency that human being always tries to do things in a simple fashion without giving much work to his brain. This is true in case of choice of passwords as well. In order to make it more simple and memorable, the user chooses passwords which are easy for him to remember but can be cracked by an adversary with less effort. That is to say, security measures are totally neglected, mostly due to ignorance or negligence or lack of knowledge. As a result, a number of online problems like password theft, guessing attacks, denial-of-service attacks, stolen-verifier attacks etc. happen. But unfortunately most of the users are totally unaware of these attacks. They have least idea that the mentioned attacks can happen to their accounts as well! As a result, security measures are usually overlooked. It is not that users are ignorant always but at times they simply ignore because they don't want to put more pressure on their brains! Users are never motivated to behave in a secure manner. So, making users aware about these matters is of at most importance today.

The best password practice of choosing passwords is mix of alphabets, numbers and special symbols. Only the online banking sites and popular sites like eBay and yahoo are making mandatory rules for choosing such passwords, while many other sites are making no restrictions on the style of the password. Many e-commerce websites are still not enforcing strong password practices [13].

In our survey, we have found that most of the websites do not provide guidelines to the user to choose a secure password. The popular social networking website, Facebook provides the following guidelines but not at the time of registration. It shows the following guidelines at the time of resetting the password.

1. It should not contain your name.
2. It should not contain a common dictionary word.
3. It should contain one or more numbers.
4. It should have both upper and lower case characters.
5. It should be over 8 characters long.
6. It must be different from your old passwords.

Similarly different websites follow different guidelines. Some other essential guidelines for best password practices [15, 18] are:

1. Use virtual keyboard for entering the credentials where the security is very important like in using online banking services.
2. Do not write your password anywhere.
3. Keep changing your password regularly in certain intervals of time.
4. Do not share your password with anyone; in case shared change the password immediately.
5. Do not choose the same password for all of your accounts.
6. Maintain your password at least 6 to 8 characters long as small length passwords are easy to crack.

Observing the results, it is clear that best password practices for online services are not being followed. The users must be guided properly in choosing secure password during the registration phase itself, and most importantly, awareness must be created among them regarding the necessity of such measures. Systems must spread the word among its users about various online attacks so that users can take such matters more seriously. Changing passwords at regular intervals of time must be made mandatory at least in online banking sites.

In Italy, the use of passwords has even become a matter of law; with privacy legislation laying down some minimum requirements (including that, where permitted by the system, they should be at least eight characters long, and be changed every six months) [7]. Likewise, it would be fruitful if all the websites follow some standard rules, procedures and enforce restriction on user so that he/she chooses a secure password.

6. Conclusion

Observation reveals that more secure mechanisms are necessary to improve the security of existing practices. The password resetting methods can be improved by adding extra layer of authentication like mobile verification and answering security questions (really secure questions!). Another recent trend is pattern unlock which is used widely. But this is confined to mobile devices. Other than this, recently picture passwords have been introduced which seem to be easily memorable. These can be utilized in a better way along with traditional techniques to make transactions or services more secure.

When all these steps have to be undertaken by the systems and sites, it becomes necessary for users to take least possible care. The user only has to use a bit of brains and tactics, spend little time over the safety measures, understand the danger they are in the present scenario due to negligence/ignorance, follow the guidelines and then choose a password. This is the least work a user can do and if done, one can clearly see the security of his/her account.

References

[1] Electronic frontier foundation, https://www.eff.org/effector/3/1

[2] S. Furnell, "An assessment of website password practices", *Computers & Security*, vol. 26, No.7-8, pp. 445-451, 2007.

[3] W.j. Haga, Zviran, "M. Question-and-answer passwords: An empirical evaluation", *Information Systems*, vol. 16, No.3, pp335-343, 1991.

[4] http://en.wikipedia.org/wiki/Ophcrack

[5] http://ophcrack.sourceforge.net/

[6] A. Adams, M.A. Sasse, "User are not the enemy", *Communications of the ACM*, Vol. 42, No.12, pp. 40–46, 1999.

[7] "See Technical Specifications Concerning Minimum Security Measures (Annex B) in Italian Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003", http://www.privacy.it/privacycode-en.

[8] "Worst passwords of 2012- and How to fix Them", SplashData, http://splashdata.com/press/PR121023.htm

[9] S. Furnell, "Getting past passwords", *Computer Fraud & Security*, Vol. 2013, No.4, pp. 8-13, 2013.

[10] Password hacks show major sites are vulnerable, *Computer Fraud & Security*, Vol. 2012, No.6, pp. 1, 3, 2012, doi:10.1016/S1361-3723(12)70057-X

[11] B. Schneier, Real-World passwords. Blog: schneier on Security, http://www.schneier.com/blog/archives/2006/12/real world_passw.html

[12] B. Schneier, Passwords are not broken, but how we choose them sure is. The Gaurdian. http://www.guardian.co.uk/technology/2008/nov/13/internet-password

[13] P. Hunter, "Vunerable websites under attack", *Computer Fraud & Security*, Vol. 2006, No.6, pp. 16-17, 2006.

[14] D. Nelson, Kim-Phuong L. Vu, "Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords", *Computers in Human Behavior*, Vol. 26, No.4, pp. 705-715, 2010.

[15] E.F. Gehringer, "Choosing passwords:security and human factors", *Technology and Society, 2002. (ISTAS'02). International Symposium,* pp. 369-373, 2002.

[16] J. Yan, Alan *et al.*, "Password memorability and security: empirical results", *IEEE Security and Privacy*, vol.2, No.5, pp. 25–31, 2004.

[17] Kim-Phuong L. Vu, R. W. Proctor, Abhilasha Bhargav-Spantzel, Bik-Lam (Belin) Tai, J. Cook, E. E. Schultz, "Improving password security and memorability to protect personal and organizational information", *International Journal of Human-Computer Studies*, Vol. 65, No.8, pp. 744-75, 2007.

[18] Common Password Mistakes and Tips for Creating Stronger Passwords, http://blogs.quickheal.com/wp/common-password-mistakes-and-tips-for-creating-stronger-passwords

[19] Designing Good Security Questions, http://goodsecurityquestions.com/designing.htm
[20] S. Schechter, A. J. Bernheim Brush, and S. Egelman, "It's no secret: Measuring the security and reliability of authentication via 'secret' questions", *IEEE Symposium on Security and Privacy, 2009*

Dr. R Madhusudhan received his M.Tech Degree in 2003 from NITK Surathkal, (A Deemed University) and PhD from IIT Roorkee in 2013. He is currently an Associate Professor in the department of Mathematical and Computational Sciences at NITK, Surathkal, India. He teaches several courses such as Computer Networks, Internet Technology and applications, Database Management Systems. He is life member of Computer Society of India and Indian Society for Technical Education. He is also a member of ACM and IEEE. His current research includes network security, remote user authentication and mobile computation.

Chaitanya S. Nayak received her M.Sc. degree in Mathematics in 2014. Presently, she is a research scholar in the Department of Mathematical and Computational Sciences at NITK, Surathkal. Her research is focused on remote user authentication and network security.