ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

SECURE PASSWORD SELECTION METHOD

Abhishek Kajal

Dept. of Computer Science & Engineering, VDIET, Julana, Jind.

Abstract- There is many things that are well known about passwords such as that user can't remember strong passwords and that the passwords they can remember are easy to guess. Our current research is examining the problem of password selection & memorability through the exploration of various password selection mechanisms. The goal of this research is develop both principles & design that help users to choose passwords that are secure and memorable. This paper also lays attention on security issues & common threats related to password selection. Here we also conducted a survey on user based passwords commonly in practice for different websites having various password selection constraints.

1. INTRODUCTION

In present era of globalization computer users manage a large number of online accounts that require passwords. Each system may have different rules for what passwords are acceptable and what passwords are not. Conventional wisdom seems to have concluded traditional passwords are inherently insecure. E mail websites have been majorly affected by the improper password selection method which results unauthorized entry to the users personal mail account. The password strength matters a lot to counter the security issues. The shortness & simplicity of passwords means many users selects credentials that will make them susceptible to basic brute force password attack. Due to limitations of human memory there occurs many deficiencies of password authentication system if humans were not required to remember the password, a maximally security password would be one with maximum entropy; it would consist of a string as long as the system allows consisting of characters selected from all those allowed by the system and in a manner that provides no redundancy.

2. Analysis of Existing Password Selection Mechanism

A good password should aim to be reasonably long large character set & still be easy to remember. There are some sublets about if the hacker has obtained a copy of password file to crack it offline or try many passwords over a network. Some sites on the web advice new users for choosing good password whereas other sites didn't provide the importance of memorability the password; just concentrate on resistance the brute force search.

2.1 Recommendations by NASA

NASA provides following suggestions for strong password selections. The ADC [1] used NASA's standards to help benchmark consumer password selection:

(a) Password should contain at least Eight Characters.

The ADC analyses revealed that just one half of the passwords contain seven or less characters.

(b) Password should contain a mix of four different type of characters as uppercase & lowercase letters, numbers and special characters such as !@#$%^&*.

The ADC analysis showed that almost 60% of users choose their passwords from within a limited set of character. About 40% of the users use only lower case character for their passwords.

(c) Password should not be a name, a slang word or any word in the dictionary. It should not include any part of your name and E mail address.

Almost all of the 5000 most popular passwords, that are used by a share of 20% of the users, were just that- names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys and so on).

2.2. Random Password Selection

Use the output from a Random password generator to select a random string that can be pronounced and is easy to remember such as the random string 'pdolisa' which can be pronounced easily use uppercase letters to create our own emphasis as 'pDOlisa'. The wider the variety of random characters with numbers and special characters make passwords much better.

2.3. Mnemonic Phrase based Passwords

Some systems try to make password selections easier by instructing user to create mnemonic phrase based passwords [2]. Choose a password that is hard for other people to guess but easy to remember by doing the following:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

1) Think of memorable sentence or phrase containing at least 8 words.

2) Select a letter, number or special character to produce new password. Use of the first letter of every word is a common practice.

3) Mixing of upper & lower case letter, numbers, punctuation & special characters.

4) Remember the phrase.

Some example of mnemonic phrase & their derived passwords are shown in table 1.

TABLE 1

Phrase	Password
In Two Thousand Twelve December me & spouse visited Goa	I3TDm&svG
I love to watch cricket match between India & Pakistan	Il2wcmb/wI&P
Jan Lokpal Bill initiated by Anna in August 2011	JLBibAiATZOO

Assumptions about mnemonic passwords are that such passwords are stronger than regular passwords as space of possible phrases is infinite and they don't appear in any password cracking dictionary.

2.4. Color implemented Password [3]

The password must not only comply with eight character scheme, but also color coding [4] pattern could be much secure. Basic colors are adopted for strengthen the password so as user have to select basic colors of the fonts too used in the password. The basic colors of Red, Black & White won't increase the size of the website & even these basic colors reduce the security threats and identity thefts which may helpful in minimizing unauthorized access of credit card hackers.

Virtual Keyboard [5] can also be made into use by making it color adaptable as virtual keyboard helps to protect the account from hacking programs. Hacking issues can be minimized even if multiple hacking programs [6] run as it's only the eye of the user which can see the color of the password fonts.

3. Common Attacks against Passwords by Hackers

This section discusses common threats against the confidentiality of passwords. Recently in December 2009, a major password breach occurred that led to the release of 32 million high volume of real world password as never before [7, 8]. Further the hackers posted to the internet [9] the full list of 32 million passwords those were stored in text database and were extracted through SQL injection vulnerability [10]. Just 10 years ago hacked hotmail passwords showed little change what reflects users choose very weak password even for sites that holds their most private data. Worse as hackers continue to rapidly adopt smarter brute force cracking software, consumers & companies will be at greater risk. For the purpose of the discussion, the threats are divided into some groups [11]: threats that directly capture passwords, such as installing key loggers [12]; threats that take advantage of weak passwords and password hashes, such as password guessing & cracking; threat that replace passwords; and threats that involve attackers reusing compromised passwords. Attackers generally compromised passwords in following ways:

1) *Password Capturing*: In capturing an attacker acquiring a password from storage transmission for user knowledge & behavior.

2) *Password Guessing & Cracking:*

Cracker attempts to determine weak passwords & to recover passwords from password hashes through techniques guessing and cracking. Guessing involves repeatedly attempting to authenticate using default passwords dictionary words and other possible passwords. It can be a brute force attack, dictionary attack or a hybrid attack. Another form of guessing attack is to search the victim's information for possible password content such as family member name or birthdates. Cracking is the process of an attacker recovering cryptographic passwords hashes and using various analysis methods to attempt to identify a character string that will produce one of these hashes, thereby being the equivalent of the password to the targeted system.

3) *By Social Engineering*:

Besides other attacks on passwords, attackers use tricks with users to reveal their username and/or passwords. Attackers captures user's password by using soldier surfing or spyware.

4. Experimental Study

In above section of Paper we have discussed different Password Selection Methods & common threats to security of passwords. In order to investigate the trade-off factors in a real context of use & to assess the passwords that users create, a survey is conducted to collect a sample. Its results compared the effect of giving alternative forms of suggestions about password selection, memorability & security. This survey includes all types of users for generating a random sample includes students, employees & other volunteers as well in both online & offline mode as per

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

individual convenient. In our survey we asked users to create passwords with some non enforced recommendations. Because we wanted to judge the quality of the passwords that participants created, we needed access to participants' clear text passwords. Thus, we instructed participants not to provide a password (or a variant of a password) that they currently use or have previously used for another account. We also asked to participant about their password selection and password management.

5. Experimental Results

Passwords generated by survey participants were analyzed using different password cracking methods such as control passwords were matched against English Dictionary & mnemonic phrases were matched against system generated mnemonic dictionary. Mnemonic Dictionary includes existing popular phrases derived from rhymes, books, movies, songs, slogans etc. readily available on internet. This way we analyzed the strength of passwords.

Not surprisingly more passwords were cracked generated for networking sites, E mail sites rather than passwords generated for Financial Institutions such as Banking A/c; Online Trading by same participant reflects user's emphasis on password strength variations for different sites. Next, participants engaged in jobs feed strong password than others as students whereas students leads in memorability of passwords. 70% Student used mostly mnemonic phrase password based on songs, rhymes & other common phrases easy to crack using mnemonic phrase dictionary. This hypothesized that users would select phrases that are publically well popular & readily available. It assists the user to easily memorize / recall a phrase rather to think a new one. Hence attracts the attacker in collecting more phrases of movies, songs, rhymes etc to crack the user's password based on mnemonic phrase what results stronger than control passwords.

6. Discussions

This study confirms some beliefs about passwords such as Mnemonic passwords are tougher to crack than regular selected passwords. Secondly it was confirmed that to keep remember different passwords for various sites is difficult as 35% participant preferred same password for all websites. Finally it is revealed that password education is having some effect on user's behaviour for selecting a strong password. Memorability is not considered the primary concern in lieu of password security as users write down their different passwords used for various online sites.

7. Conclusion

User needs to create strong password for sites storing their private information as "Take a sentence and turn it into password". As "CBI should be kept under LokPal" might become "CBIsbkuLP" which doesn't exist in anyone's dictionary.

Users need to generate different passwords for various sites even if privacy isn't a big issue. If memorability is a concern for many passwords, write down hints / sentence for all & keep with self. Users shouldn't trust 3rd party for important passwords as banking etc.

From administrative point of view, administrator needs to enforce strong password policy so as users wouldn't able to select weak password. Employ aggressive anti brute force mechanisms to detect brute force attacks on login credential. Administrators need to make sure that password are not kept or transmitted in clear text. Enhance password change policy & encourage passphrases instead of regular password as former may be stronger to crack after adding characters.

References

[1] http://www.hq.nasa.gov/office/ospp /securityguide/V1comput/password.htm
[2] Kuo, Cynthia; Romanosky, Sasha; and Cranor, Lorrie Faith, "Human Selection of Mnemonic Phrase-based Passwords" (2006). Institute for Software Research. Paper 36 http://repository.cmu.edu/isr/36
[3] Akash Mathur,"Improved Password Selection Method to Prevent Data Thefts",*International Journal of Scientific & Engineering Research"* volume 2, Isuue 6, June 2011.
[4] L Cottrell, L M Cottrell, "*HTML & XHTML Demystified"*, USA: The McGraw Hill companies, pp. 50-56, 2011
[5] M Hirose, *Human-Computer Interaction Interact-'01," Netherlands: IOS Press, pp. 678-679, 2001.*
[6] S Mclure, J Scambray, G Kurtz, *"Hacking Exposed" 5th* Ed. USA: McGraw Hill/Osborne, 2005.
[7] http://blog.absolute.com/passwords-are-not-enough/
[8] http://www.rockyou.com/help/ securityMessage.php
[9] http://igigi.baywords.com/rockyou-com-passwords-list/
[10]http://www.techcrunch.com/2009/12/14/rockyou-hacked/
[11]Karen Scarfone, Murugiah Souppaya, *"Guide to Enterprise Password Management (Draft)",* US Department of Commerce, NIST, Special Publication 800-118
[12]R.C Newman, "*Computer Security-protecting digital resources",* Jones and Bartletts publishers, pp. 58-59, 2009