

|  |  |  |
| --- | --- | --- |
| MSc Advanced Software Engineering  Research Project | | |
|  | | |
| Assignment Type: | Literature review | |
| Submission Date: | 01/31/2017 | |
|  | | |
| Student Id | | Student Name |
| 2015101 | | K.A.S.C.Kathriarachchi |

|  |
| --- |
|  |
| Literature Review |
| Blocking brute force attacks using binomial ladder filter in .net applications |

Student Id - 2015101

Name - K A S C Kathriarachchi

Supervisor - Mr Cassim Farook

**Table of Contents**

* Abstract 4
* Introduction 4
* Password attributes - Literature Review 7
* Research Method 13
* Findings 13
* Discussion 14
* Conclusion 15
* Reference 16
* Other Information Sources 16

**Abstract**

Password-based systems and, more generally, authentication systems based on *something you know*, are commonplace on the Internet. Web applications using these systems can be the target of brute force login attacks, in which an attacker tries to compromise a given account or any user account on the system. These applications rarely implement effective protection mechanisms against these attacks. In this paper, we review the other researches relating to this project.

**Introduction**

Password-based authentication mechanisms are both extremely common and highly criticized in the world of computer systems. They are criticized because they do not provide adequate protection in practice. For example, in Bishop and Klein, reporting on an experiment conducted in the late 1980s, explained how they attempted to crack a set of nearly 14,000 real Unix passwords gathered from various sources. To perform their attack, they used a variety of brute force methods and some more adaptive techniques. They report that they were able to crack about 3.2% of the password set in the first 15 minutes, and that they cracked about 40% of the data set in about three CPU years (about 21% of them in the first week). Their result confirmed the already well known fact that human users tend to pick poor passwords (in that these passwords are relatively easy to guess), as documented, for example, in the late 1970s by Morris and Thomson. However, in retrospect, these early results were in fact encouraging, even though they were not presented as such by the authors. Indeed, for example, Bishops and Klein were able to crack *only* 40% of the passwords in 3 CPU-years! The main conclusion that could be drawn at the time was that passwords as such were fine, as long as “good ones” were chosen.

Unfortunately, the situation has become significantly worse since then: despite years of user education, strong evidence shows that end users still tend to use easy-to-guess passwords. It is difficult to blame end users for this, since the number of passwords to remember has ballooned to several dozen for a typical user, making it very impractical to expect people to pick hard-to-guess, yet memorable, passwords for so many accounts. But the main problem lies with password cracking techniques and computer speed. It is very likely that Bishop and Klein would now successfully guess the vast majority of their database, and do so in much less than three CPU years. It is also the case that they would have easy, cheap access to a lot more than three CPU years to run their attack if they wished. It can be argued, and it sometimes is, that the times when it was possible to create a password that a human can remember and that a determined, well equipped attacker cannot crack are behind us.

Even though password-based authentication systems are known not to provide very good security, they are still very popular, and represent the vast majority of authentication systems that are deployed currently. The reasons for this are simple: despite its poor security value, a password-based authentication mechanism is very easy to deploy, does not require any additional hardware, and is well accepted amongst the potential user population. It is arguably the simplest, most cost effective solution to use when you have to authenticate users with some minimal level of security. Because of this, these systems appear to be here to stay.

This bleak situation may not be as bad as it first seems. It is true that password-based authentication mechanisms do not provide adequate protection against well-equipped attackers, but this analysis is based on so-called “offline” attacks, in which the attackers have direct access to some encrypted version of the passwords. In this situation, the only thing that slows down the attack is the generation of encrypted passwords on the one hand, and the comparison of the result with the list on the other hand. Thankfully, this situation is not the most common one. If we assume that the attacker does not have access to the database of passwords directly, then the attack must be performed online, through the system’s legitimate gateway. The situation is very different in that case: for one thing, it is likely much slower, and for another thing designers of the system have an opportunity to act against such attacks.

(e.g., by slowing them down or by stopping them completely). In fact, in a recent paper published in 2007 tellingly titled “Do strong web passwords accomplish anything?”, Florêncio, Herley and Coskun point out that very little actual entropy is required to adequately protect Web applications as long as the right mechanisms are in place on the server side to prevent brute force attacks . Unfortunately, one can fairly assume that for most current Web applications, the desired “right mechanisms” are actually not in place.

In this paper, we try to address this situation: we define what properties such a mechanism must possess, and we then propose a very simple solution, along with an implementation in .net. my solution is meant to enhance very significantly the security of Web applications when it comes to protecting against online brute force attacks, and is designed in such a way that it can be easily integrated into both new and existing systems.

The paper is organized as follows: in Section II, we review the situation as it is currently: the types of attacks Web application are facing in the area of brute force attacks, the types of protections that are typically in place and their shortcomings, and what would be required for a good protection system. In Section III, we provide an overview of our proposed solution, as a combination of three simple ideas: separate the protection from the authentication; apply protection along all possible entry points; and use a sliding window approach when protecting. We describe an implementation of our system in Section IV, and we discuss the strengths and weaknesses of our solution in Section V.

**Password Attributes**

Zviran and Haga (1999) conducted a survey on computer users at a Department of Defense installation in California. Questionnaires were returned by 997 participants. Zviran and Haga (1999) observed that 24.9% of the respondents had 6 characters in their passwords.

Zviran and Haga (1999) also observed that 80.1% of the respondents’ passwords consisted of only alphabetic characters.

Zviran and Haga (1999) observed that most user-selected passwords are derived from the characteristics of personal details meaningful to the individual, are fairly short, are made up of alphanumeric characters, are seldom changed, and are frequently written down. In other words, passwords remain easy to memorize and simple in structure and construction. Zviran and Haga (1999, p.179) observed the following:

1. Password selection methods affect password memorizability.
2. The increased frequency of changing a password, even though it increases the level of security, hinders memorizability.
3. The more frequently a password is used, the less often it is written down.
4. The more a password is used, the less difficult it is to remember.
5. Changing passwords frequently, although necessary to reduce password predictability, hinders recall.
6. Difficulty recalling a password is related to a user's tendency to write it down.
7. Difficulty recalling a password or writing it down is not related to a password's length.
8. Whether a password was chosen to make it easy to remember has no bearing on whether it is written down.

Zviran and Haga (1999) urge replication of their findings in future research to challenge these findings in various user populations and organizations to enhance their generalizability.

When users are allowed to select their own passwords, they tend to select passwords that are easy to remember but also easy to crack (Adams & Sasse, 1999). End users prefer passwords that are short, simple, and derived from meaningful details (Adams & Sasse, 1999). Like Zviran and Haga (1999), Adams and Sasse (1999) observed that some users create their passwords based on details meaningful to them. This potentially includes variations of their own or a relative’s name, a pet’s name, street address, birth date, social security number, etc. (Adams & Sasse, 1999). They also observed that user knowledge regarding secure password content is not sufficient (Adams & Sasse, 1999). Most end users do not know how to create a secure password, and they do not know how serious it can be if their passwords are compromised (Adams & Sasse, 1999).

Adams and Sasse (1999) posit that, without instruction from IT experts, end users often create their own rules for inventing passwords, which are thus often not secure. Passwords that can be

**The following table summarizes the literature review related to end-user behavior in the utilizations of passwords:**

|  |  |  |  |
| --- | --- | --- | --- |
| Study | Regarding the study | Method | Results |
| Zviran, M., and Haga, W.J. "Password security: An empirical study," Journal of Management Information Systems 1999 | The paper addresses the gap in evaluating the characteristics of real-life passwords and presents the results of an empirical study on password use. The paper investigates the core characteristics of user-generated passwords and associations among those characteristics. | The researchers conducted questionnaires on computer users at the Department of Defense in California. Users returned 997 questionnaires | 1 Password selection methods affect password memorizability.  2. The frequency of changing a password hinders memorizability.   3. The more frequently a password is used, the less often it is written down.   4. The more a password is used, the less difficult it is to remember.  5. Changing passwords frequently hinders recall.  6. Difficulty recalling a password is related to a user's tendency to write it down.  7. Difficulty recalling a password or writing it down is not related to a password's length.  8. Whether a password was chosen in such a manner as to make it easy to remember is not related to whether it was written down. |
| Sasse, M.A., Brostoff, S., and Weirich, D. "Transforming the 'Weakest Link' -- a Human/ Computer Interaction Approach to Usable and Effective Security," *BT T echnology Journal* 2001 | The researchers investigated the behaviors of users regarding the use of passwords. The researchers concluded that undesirable behaviors associated with the use of passwords originate from the failure to understand the attributes of memorizability, incompatible task demands, and lack of training, support, and proper motivation. | The researchers conducted a qualitative study using questionnaires and in-depth interviews among users. | 1. The frequency of using passwords can positively affect memorizability.  2. Passwords that require100% accurate recall are not good for infrequently used systems.  3. Heavily or frequently used passwords are more regularly confused than infrequently used passwords.    4. Recalling robust passwords that are rare or non-meaningful is an impossible task for humans.  5. People who have a strong password are viewed as “paranoid” or “antisocial”.  6. Sharing passwords is considered a sign of trust among colleagues and friends.  7. Most users underestimate the potential damage caused by compromised. passwords. |
| Warkentin, M., Davis, K., and Bekkering, E. "Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security," *Journal of Organizational and End User Computing* 2004 | The study proposes that the Check off Password System (COPS) is more secure than self- selected passwords. The study analyzes the differences between using COPS and three traditional password procedures. | The researchers conducted a control experiment. There were 352 participants, all college students. | The study indicates that COPS is a better alternative to current user authentication method. The study suggests that end users perceive all password procedures tests to have equal usefulness; however, the perceived ease of use of the COPS method is equivalent to an established high security password, and the COPS interface does not negatively affect user performance compared with that of a high security password. |

**Research method**

The survey was used to analyze the current characteristics of users’ behavior in utilizing their passwords this will act major analysis for my project on stop bruit force attacks using binomial ladder filter.

**Findings**

Passwords are still one of the weakest links in information systems because people use weak passwords. According to the survey, nearly eighty percent of users have fewer than ten characters in their passwords, and more than half of the respondents reported having only characters in their passwords. With the current password-cracking software, these passwords are easy to crack in a matter of seconds. The results of this study also show that people often create passwords based on their personal information such as birthdates, citizen id, telephone number, and family members’ names. These passwords can be easily guessed by friends and colleagues. Another problem that I observed in the results of this study is people often reuse passwords. Nearly everyone in the study reported that they have only between two and three passwords to access every account. This can lead to the domino effect problem in which the hacker can gain access using one password and then use the same passwords for other accounts. Sometimes, the hackers do not even need to hack the password. They can set up a website and ask users to register with a username and password. Some people will reuse the same password that they use with other accounts such as email, their company’s systems, and e-banking accounts. Once the hacker has a user’s password, he or she can use the same password with other systems including users’ email and e-Banking account.

According to analysis we need an additional system to prevent attacks to the systems, because most of the peoples using easily hackable passwords.

**Discussion**

In this study, the results present the contrast between strong passwords and memorization. Miller (1956) posits that human short-term memory can store only seven plus or minus two chunks of information (Miller, 1956), and unless a person develops a systematic way to memorize that information, it will be forgotten in less than 30 seconds (Higbee, 2001). This finding is consistent with the research documents used in creating the study, indicating that the longer a password is, the more difficult it is to remember (Sasse et al., 2001; Schneier, 2000; Warkentin et al., 2004; Zviran & Haga, 1999). When the users cannot memorize the passwords, the solution is for them to write the passwords down. In this study, nearly half of the respondents indicated that they wrote down their passwords to aid their password memorizability.

Sharing passwords is common practice in IS organizations (Sasse et al., 2001). Passwords are supposed to be secret; thus, sharing them defeats the purpose of having them, making it next to impossible to verify who the users are in the system or to account for what went wrong with the system (Sasse et al., 2001). The main reason users share their passwords is for convenience. In this study, the results indicate that nearly half (43%) admitted that they have shared company passwords with friends or colleagues. Finally, the results indicate that most users never change their passwords. This can create a serious problem because most users do not know if their passwords have already been compromised. The hacker can use compromised passwords to access users’ accounts without the users’ knowledge.

**Conclusions**

Passwords are the first line of defense in any information system; however, their importance has been ignored by both practitioners and researchers. The literature related to password security indicates that a strong password that is long, complicated, and not derived from personal, meaningful details is difficult to remember and weak passwords that are short, simple, and derived from personal, meaningful details are easy to remember (Schneier, 2000; Warkentin et al., 2004; Zviran & Haga, 1999). When users cannot memorize a password, the solution is to write it down (Sasse et al., 2001; Schneier, 2000; Zviran & Haga, 1999). A written password can be lost or stolen. In addition, when users cannot memorize numerous passwords, they often reuse the same password multiple times. If hackers can gain access to one account, they may be able to gain access to other accounts (Ives et al., 2004). Memory literature indicates that humans have a limited capacity for memorizing information (Higbee, 2001; Miller, 1956). Information stored in long-term memory can be memorized for a longer period than information stored in short-term memory (Higbee, 2001). The findings of this study support previous findings in the literature that end users use weak passwords. The majority of users write down their passwords. Most users reuse a password for multiple accounts. Most users share their passwords and never change them. IT security must develop both technical and policy solutions to address the problems of users’ behavior in utilizing passwords; otherwise, passwords will continue to be a weak link in information systems. We need secondary solution to protect systems on these guessing attacks.

**References**

1. Zviran, M., and Haga, W.J. 1999 "Password security: An empirical study,"
2. Sasse, M.A., Brostoff, S., and Weirich, D. 2001 "Transforming the 'Weakest Link' -- a Human/ Computer Interaction Approach to Usable and Effective Security,"
3. Warkentin, M., Davis, K., and Bekkering, E. 2004 "Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security,"
4. Lars R. Knudsen[,](mailto:lars.r.knudsen@mat.dtu.dk) Matthew J. B. Robshaw series 2016 “Information Security and Cryptography”
5. Marc Cameron 2015 “Brute Force (Jericho Quinn Thriller Book 6) “
6. Matt Curtin 2005 “Cracking the Data Encryption Standard”

**Other Information Sources**

1. Wikipedia about brute force attacks - <https://en.wikipedia.org/wiki/Brute-force_attack>
2. Wikibooks Cryptography>Brute\_force\_attack - <https://en.wikibooks.org/wiki/Cryptography/Brute_force_attack>