Shadow Attacks based on Password Reuses: A Quantitative Empirical Analysis

**ABSTRACT**

With the proliferation of websites, the security level of password-protected accounts is no longer purely determined by individual ones. Users may register multiple accounts on the same site or across multiple sites, and these passwords from the same users are likely to be the same or similar. As a result, an adversary can compromise the account of a user on a web forum, and then guess the accounts of the same user in sensitive accounts, e.g., online banking services, whose accounts could have the same or even stronger passwords. We name this attack as the shadow attack on passwords. To understand the situation, we examined the state of- the-art Intra-Site Password Reuses (ISPR) and Cross-Site Password Reuses (CSPR) based on the leaked passwords from the biggest Internet user group. With a collection of about 70 million real-world web passwords across four large websites in China, we obtained around 4.6 million distinct users who have multiple accounts on the same site or across different sites. We found that for the users with multiple accounts in a single website reused their passwords and for the users with multiple accounts on multiple websites reused their passwords across websites. For the users that have multiple accounts but different passwords, the set of passwords of the same user exhibits patterns that can help password guessing: a leaked weak password reveals partial information of a strong one, which degrades the strength of the strong one. Given the aforementioned findings, we conducted an experiment and achieved an improvement of guessing success rate with John the Ripper guessing tool. To the best of our knowledge, we are the first to provide a large-scale, empirical, and quantitative measurement of web password reuses, especially ISPR, and shed light on the severity of such threat in the real world.

SYSTEM ANALYSIS

EXISTING SYSTEM:

 Existing password schemes, many voices have called for password replacement or enhancement. Described many ancillary means to replace the current password-based authentication mechanism. Existing that a user should group their accounts when he or she has many different passwords.

PROPOSED SYSTEM:

 Proposed that a user should reuse their passwords in similar accounts, because they argue that it is impossible for a user to remember so many passwords, and input them in correct user interfaces. They proposed that each attack method has its strength in cracking passwords of certain strength. They also pointed out that the probability of guessing a correct password will decrease exponentially as the search space grows up, which is consistent with our experiment results. Proposed that a user should group their accounts when he or she has many different passwords.

Algorithm:

Password-guessing algorithms:

 This method assumes that you can retrieve the hash of the password to be guessed and that the hashing algorithm is the same between the rainbow table and the password.

Password cracking algorithms:

 Brute Force Password Cracking Algorithm trying to write a brute force password cracker in which tests all possible alphanumerical strings of length , then all possible strings of length

Attacks:

**Phishing Attack**:

 Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

**Dictionary Attack:**

 Vulnerability to password or decryption-key assaults can be reduced to near zero by limiting the number of attempts allowed within a given period of time, and by wisely choosing the password or key. For example, if only three attempts are allowed and then a period of 15 minutes must elapse before the next three attempts are allowed, and if the password or Key is a long, meaningless jumble of letters and numerals, a system can be rendered immune to dictionary attacks and practically immune to brute-force attacks.

**Brute Force Attack:**

 Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies.

**Password Guessing Attack:**

 A common threat web developer’s face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

**SYSTEM SPECIFICATION**

**Hardware Requirements:**

* System : Pentium IV 3.5 GHz or Latest Version.
* Hard Disk : 40 GB.
* Monitor : 14’ Colour Monitor.
* Mouse : Optical Mouse.
* Ram : 1 GB.

**Software Requirements:**

* Operating system : Windows XP or Windows 7, Windows 8.
* Coding Language : Java / J2EE (Jsp,Servlet)
* Data Base : My Sql Server
* Documentation : MS Office
* IDE : Eclipse Galileo
* Development Kit : JDK 1.6
* Server : Tomcat 6.0

Conclusion:

 According to the conclusion made in prior work that the number of valid email addresses on the same website should be smaller than 25 on averages, we removed all accounts whose email addresses had been used for more than 25 times on one website. Finally, we found that and CSDN contained some accounts with the same emails and usernames but different passwords. the passwords in Disport are stronger than those in Dips against online guessing attacks. The first two metrics indicate that the occurrence of the most frequent passwords in Disport is lower than the ones in Dips. The rate of CSPR is the lowest for users with education email addresses, and the number is smaller than the general rate . This result confirms our hypotheses that users in academic organizations are better educated with web security than common users and tend to use different passwords for accounts in different websites. Another reason may be that users incline to reuse passwords when registering with low-valued or easily replaceable email accounts. Academic emails, however, are difficult to be replaced.