Conference Paper | PDF Available

# An analysis of password security risk against dictionary attacks

October 2022
Conference: The International Symposium on Information Theory and Its Applications (ISITA) - At: Tsukuba, Japan

**Authors:**

**Binh Thanh Thai Le**
National Defense Academy of Japan

**Hidema Tanaka**



Abstract

In the use of information systems, passwords are a basic means of user authentication and have an important role in practical security. Meanwhile, with the spread of various Internet services in recent years, opportunities for setting passwords are increasing. Therefore, strong passwords are always required to perform the role of user authentication, and the number of password requirements is increasing. The main topic of passwords is their quality or strength, i.e., how hard it can be guessed by an attacker, and there are various password strength meters have been proposed so far. In this study, we propose an evaluation method for password strength with the consideration of the risk of dictionary attacks and compare its effectiveness with previous PSMs. Our method uses leaked password lists as a Markov information source, and we report it as a Markov information source. Thus, we calculate the self-information of the password and use this value to show the risk of dictionary attacks or compare the strength of several passwords. By experimental results, we show that our method is very effective and can help to create effective passwords.





ISITA2022, Tsukuba, Japan, October 17-19, 2022

# An analysis of password security risk against dictionary attacks

Binh Le Thanh Thai
*Department of Computer Science*
*National Defense Academy*
Yokosuka, Japan
binhlee0430@gmail.com

Hidema Tanaka
*Department of Computer Science*
*National Defense Academy*
Yokosuka, Japan
hidema@nda.ac.jp

**Abstract—In the use of information systems, passwords are a basic means of user authentication and have an important role in practical security. Meanwhile, with the spread of various Internet services in recent years, opportunities for setting passwords are increasing. Therefore, strong passwords are always required to perform the role of user authentication, and the number of password requirements is increasing. The main topic of passwords is their quality or strength, i.e., how hard it can be guessed by an attacker, and there are various password strength meters have been proposed so far. In this study, we propose an evaluation method for password strength with the consideration of the risk of dictionary attacks and compare its effectiveness with previous PSMs. Our method uses leaked password lists as a Markov information source, and we report it as a Markov information source. Thus, we calculate the self-information of the password and use this value to show the risk of dictionary attacks or compare the strength of several passwords. By experimental results, we show that our method is very effective and can help to create effective passwords.**

## I. Introduction

### A. Background and motivation

In the field of information security, passwords are still a predominating approach for user authentication because of **usability**, **deployability**, and **security** advantages which are generating a password, security and convenience conflict [1]. For example, complex passwords that include uppercase and lowercase letters, digits, and special characters are secure but are inconvenient to use because they are very difficult to remember. However, from the viewpoint of confidentiality, it is important to choose such a strong password. Due to this fact, the main issue with the password is its quality or strength, i.e., how hard it can be guessed by an attacker. Many proposed or commercial PSMs have been proposed so far [2]–[8].

However, even if the same password is used, the password strength differs greatly depending on the PSMs. Tab. I shows the strength of the password `password1` evaluated by some service vendors [5]. From Tab. I, we can find that the password `password1` is evaluated as "very weak" by Dropbox, whereas Twitter and Yahoo! gave it a max score. This fact may make users confused whether their passwords are really strong. Solving this problem is our motivation. Moreover, password security is a relative matter, and PSMs also may be not really "strong" if it has already leaked [6]. By collecting leaked passwords and building a database, it is possible to verify whether a password has been leaked or not. With this consideration, we propose an evaluation method password strength against the risk of dictionary attacks and compare its effectiveness with previous PSMs. Our method uses leaked password lists as a Markov information source, calculates the value of self-information of the target passwords, and shows the risk of dictionary attacks.

TABLE I
EXAMPLE OF PASSWORD STRENGTH SCORE

| Service | Strength | Score |
|---|---|---|
| Google | Strong | 3/4 |
| Dropbox | Very weak | 1/5 |
| eBay | Medium | 4/5 |
| Facebook | Fair | 2/4 |
| Microsoft (US) | Medium | 2/4 |
| Skype | Poor | 1/5 |
| Twitter | Perfect | 4/4 |
| Yahoo! | Very strong | 4/4 |

### B. Password cracking methods

The well-known password cracking methods are as follows.

*1) Brute-force attack:* A brute-force attack is to use trial-and-error to check all possible passwords until the correct one is found. In theory, this method can be used to crack every password. However, since this attack method greatly relies on the computing power, it is only effective to check all short passwords. Currently, it is practically feasible to use the brute-force approach to crack only passwords with a length less than 7. In this way, the success or failure of the attack is determined by the length of the target password, so it is not the target of password strength of this study.

*2) Rainbow table attack [7]:* The rainbow table attack uses a table (a "rainbow table") to crack the password hashes. The rainbow table itself refers to a precomputed table that contains all password hash values. If attackers gain the list of password hashes, they can crack all passwords very quickly with a rainbow table. However, this method targets the hash values; thus, it is not affected by the password strength. Therefore, it is not the target of password strength.

*3) Dictionary attack [8]:* A dictionary attack is an attack using a dictionary as a set of leaked passwords. Since most