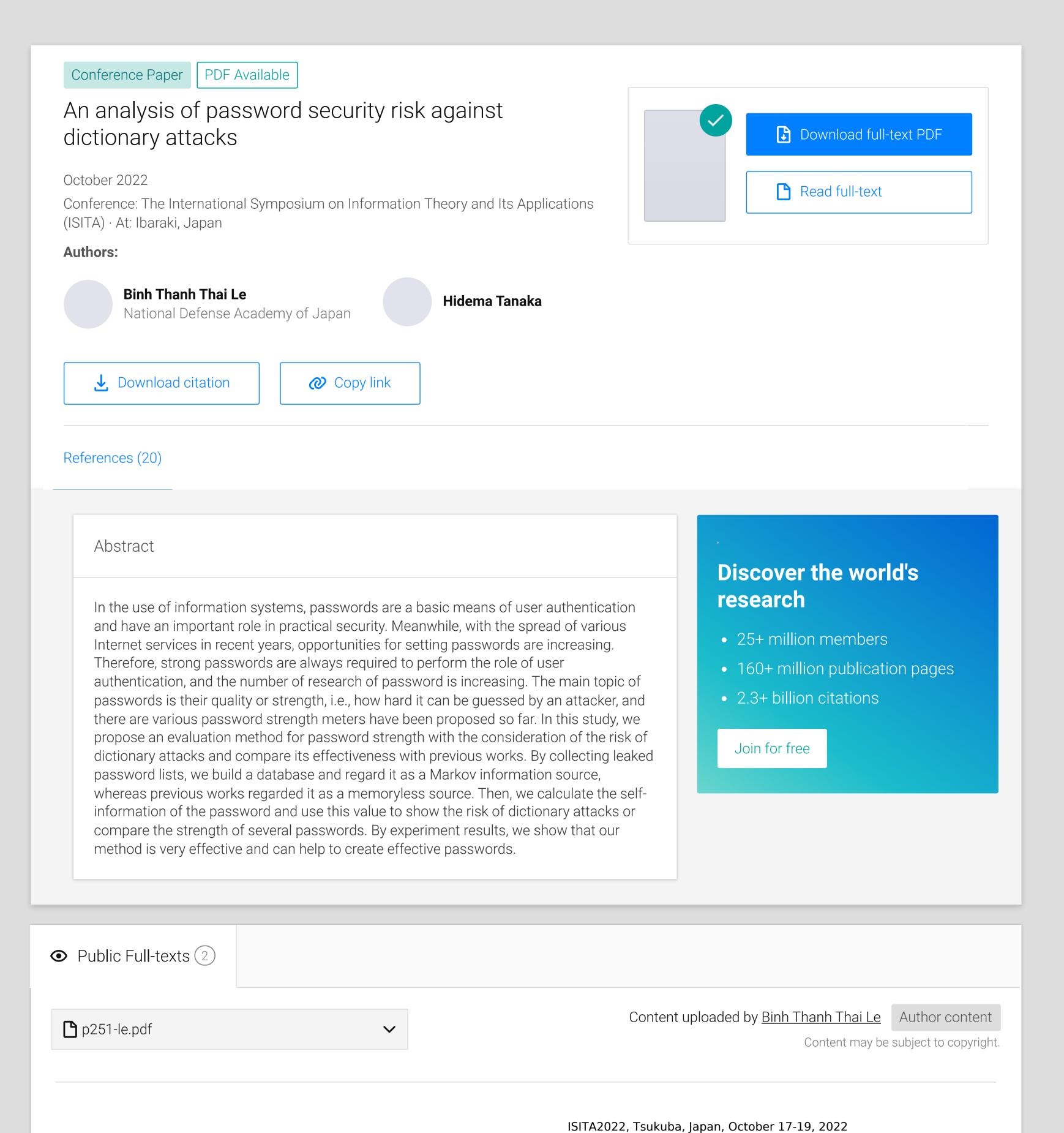
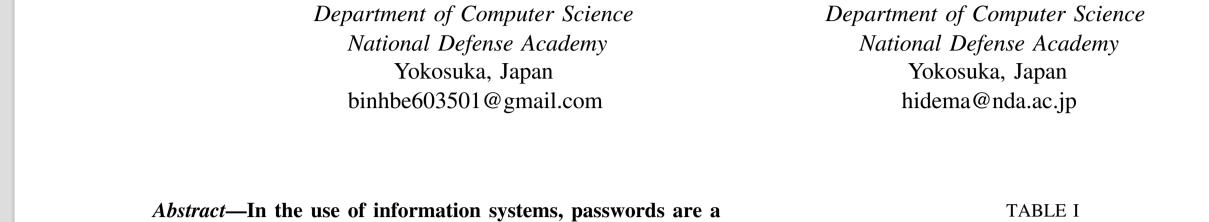
Login





Binh Le Thanh Thai

An analysis of password security risk

against dictionary attacks

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 works. By collecting leaked password lists, we build a database and regard it as a Markov information source, whereas previous works regarded it as a memoryless source. Then, 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 experiment 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 their convenient simplicity and sound implementation. When generating a password, security and convenience conflict [1]. For example, complex passwords that include uppercase and is found. In theory, this method can be used to crack every 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 the computing power, it is only effective to check all short

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 password

However, even if the same password is used, the password

strength differs greatly depending on the PSMs. Tab. I shows

strength meters (PSMs) have been proposed [2]-[4].

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

research of password is increasing. The main topic of passwords

This fact may make users confused whether their passwords are really strong. Solving this problem is our motivation. Furthermore, a password is evaluated as "strong" by some PSMs also maybe not really "strong" if it has already leaked [6]. By collecting leaked passwords and building a database, Copyright (C) 2022 by IEICE

References (20)

Article Full-text available Jan 2007

Article Jan 1995 · COMPUT SECUR

Show abstract

Matt Bishop · Daniel V. Klein

A Conceptual Framework for Assessing Password Quality

Improving system security via proactive password checking

Wanli Ma · John Campbell · Dat Tran · Dale Kleeman

Citations (0)

Service Strength Apple Moderate Very weak Dropbox Medium eBay Fair Google Microsoft (v3) Medium Skype Poor Twitter Perfect Yahoo! Very strong 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,

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

password. However, since this attack method greatly relies on

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

and shows the risk of dictionary attacks.

B. Password cracking methods

251

EXAMPLE OF PASSWORD STRENGTH SCORE

Score

2/3

1/5

4/5

3/5

1/3

6/6

Hidema Tanaka

only by the length of the password, so it is not the target of password strength of this study. 2) Rainbow table attack [7]: The rainbow table attack uses the strength of the password password\$1 evaluated by a table (a "rainbow table") to crack the password hashes. The some service vendors [5]. From Tab. I, we can find that rainbow table itself refers to a precomputed table that contains the password password\$1 is evaluated as "very weak" by all password hash values. If attackers gain the list of password Dropbox, whereas Twitter and Yahoo! gave it a max score. 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 our topic of password strength. 3) Dictionary attack [8]: A dictionary attack is an attack using a dictionary as a set of leaked passwords. Since most

```
Show abstract
Improving Password Memorability, While Not Inconveniencing the User
 Article Feb 2019
Naomi Woods · Mikko Siponen
       Show abstract
Shadow Attacks based on Password Reuses: A Quantitative Empirical View
 Article May 2016
Weili Han · Zhigong Li · Minyue Ni · Wenyuan Xu
      Show abstract
A Large-Scale Evaluation of High-Impact Password Strength Meters
 Article Jun 2015
 Xavier de Carné de Carnavalet · Mohammad Mannan
       Show abstract
From Very Weak to Very Strong: Analyzing Password-Strength Meters
 Conference Paper Jan 2014
 Xavier de Carné de Carnavalet · Mohammad Mannan
View
The Three Sigma Rule
 Article May 1994
Friedrich Pukelsheim
      Show abstract
A Mathematical Theory of Communication
 Article Jan 2001
Claude E. Shannon
View
An off-line dictionary attack on a simple three-party key exchange protocol
 Article Mar 2009
Junghyun Nam · Juryon Paik · Hyun-Kyu Kang · Dongho Won
       Show abstract
A Mathematical Theory of Communication
 Article Jan 1948
Claude E. Shannon
       Show abstract
                                                      Show more
Recommended publications
   Conference Paper Full-text available
                                                                   Chapter
```



Business solutions

<u>Advertising</u>

Recruiting

© 2008-2024 ResearchGate GmbH. All rights reserved.

Support

Help Center

A novel metric for password security risk against

Passwords are still the most used method of user authentication in the usage

of information systems, and they have an important role in practical security.

Despite the fact that researchers have discovered various vulnerabilities in the usage of passwords, this authentication method is still frequently used. The

main issue with passwords is their quality or strength, i.e., how hard they can

A statistical Markov-based password strength meter

Although multi-factor authentication is gaining popularity, password-based

PSMs still use simple rule sets or rely on heuristic results. With the

authentication remains the most commonly employed method for both online

login and data encryption. To help users choose secure passwords, password strength meters (PSMs) are a well-known and important tool. However, many

Binh Thanh Thai Le · Hidema Tanaka

dictionary attacks

be ... [Show full abstract]

Article Full-text available

April 2024 · Internet of Things

Hidema Tanaka · Binh Thanh Thai Le

continuous development of ... [Show full abstract]

August 2022

View full-text

View full-text

Company

About us

<u>News</u>

Terms · Privacy · Copyright · Imprint

A Novel Metric for Password Security Risk Against

Passwords are still the most used method of user authentication in the usage

of information systems, and they have an important role in practical security. Despite the fact that researchers have discovered various vulnerabilities in the

usage of passwords, this authentication method is still frequently used. The

main issue with passwords is their quality or strength, i.e., how hard they can

Password has been a predominating approach for user authentication to gain access to restricted resources. The main issue with password is its quality or

strength, i.e. how easy (or how hard) it can be "guessed" by a third person

who wants to access the resource that you have access to by pretending

being you. In this paper, we review various metrics of password quality,

On Password Strength: A Survey and Analysis

June 2018 · Studies in Computational Intelligence

including one we ... [Show full abstract]

Hidema Tanaka · Binh Thanh Thai Le

Dictionary Attacks

be ... [Show full abstract]

Chapter Full-text available

Gongzhu Hu

View full-text

Read more

February 2023