

Promoting Memorability and Security of Passwords Through Sentence Generation

Bik-Lam Belin Tai², Kim-Phuong L. Vu², Abhilasha Bhargav¹, and Robert W. Proctor^{1,2}

¹CERIAS, ²Department of Psychological Sciences

Aim:

Evaluate the effectiveness of a sentence generation method in recall and security.

Introduction:

The username-password combination is a widely used method of authentication and identification.

Problem:

Meaningful strings are usually generated as passwords, and these are easy to crack with programs. As a result, attackers could gain access to personal data and resources.

Solution:

Combine proactive password checking with a sentence generation method.

-Proactive password checking allows users to generate crack-resistant passwords by imposing restrictions.

-Sentence generation method requires a user to generate a sentence from which a password is formed by taking the first letter of each word. The password should be memorable because the sentence context provides recall cues.

Method:

Participants: 40 students from Purdue University

Apparatus: A java program was used

- To present instructions to participants
- To record and check the generated passwords
- To record the number of attempts and the time taken

Procedure:

- Participants were divided into 2 groups of 20.
- The experiment consisted of 3 parts:

1. Password Generation:

One group was asked to generate passwords for 3 fake accounts under 3 restrictions and another under 5 restrictions.

The password restrictions for the first group were that the sentence should:

- 1.) have at least 6 words
- 2.) make sense, and
- 3.) be unique for each account.

For the second group, the sentence should also:

- 4.) have a special character (e.g., !, @, or #) embedded in it, and
- 5.) have a digit embedded in it.

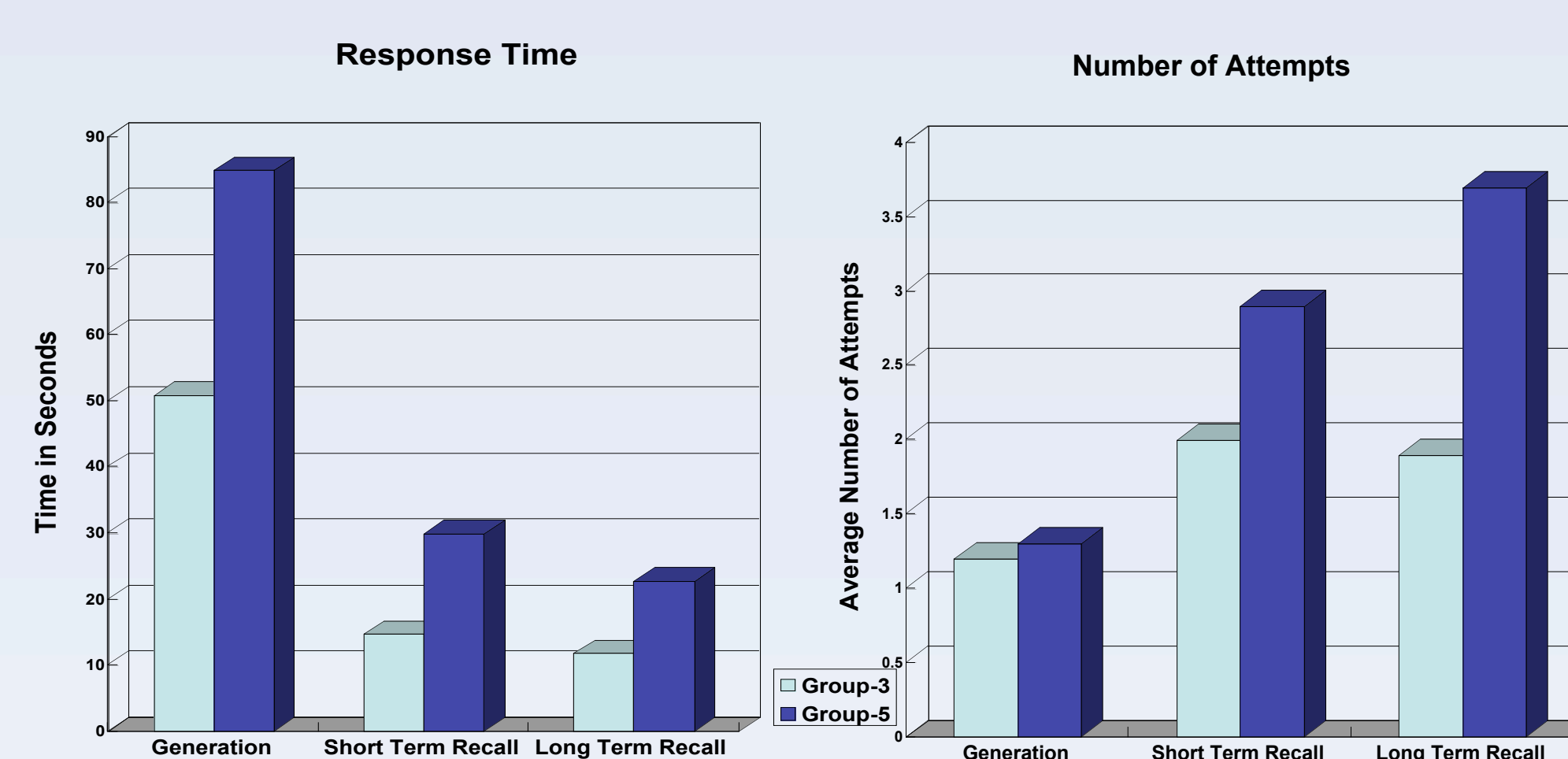
2. Password Recall

- Short-term recall: 5-minute delay
- Long-term recall: 1-week delay

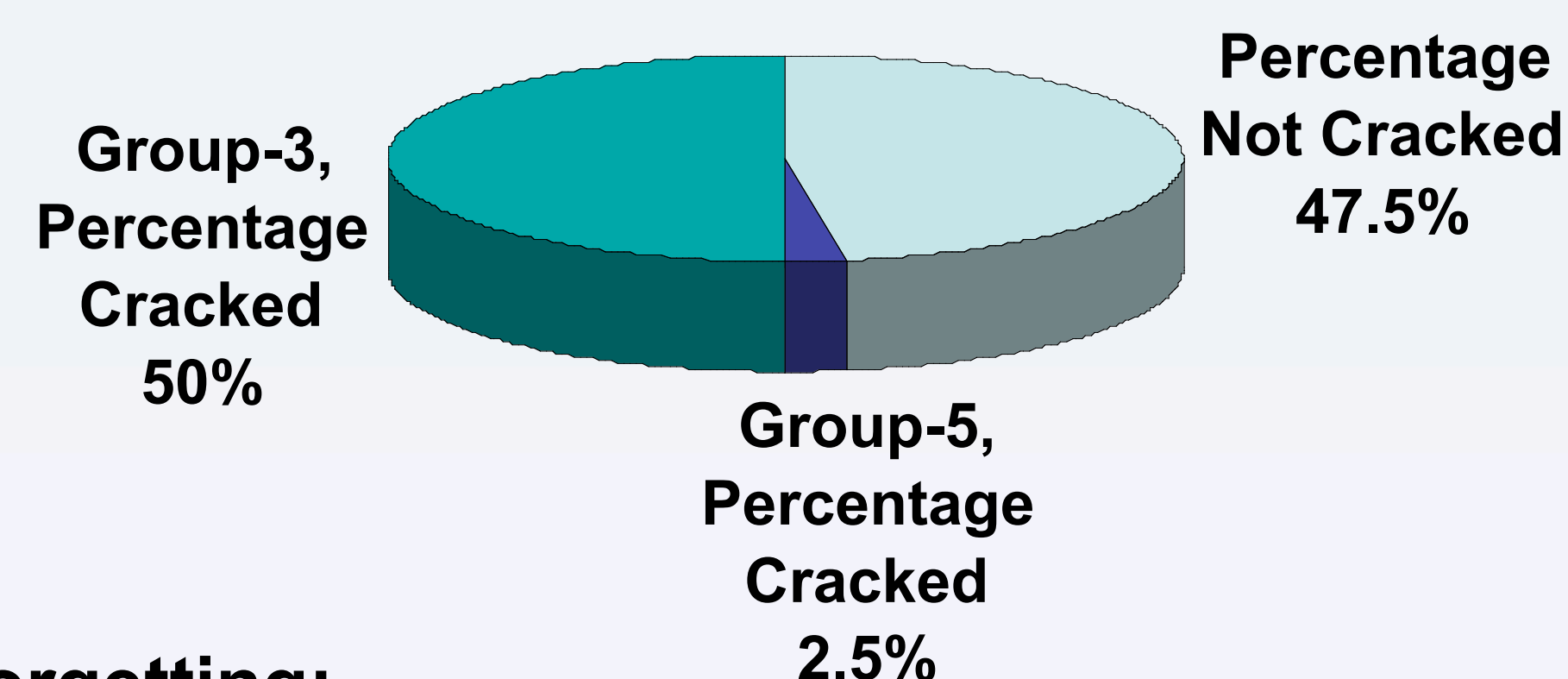
During each recall session, users logged into each account 4 times in random order.

A maximum of 10 attempts were given for each account occurrence.

Results:



Results after using LC4 for 12 hours



Forgetting:

For 3-restriction group,

- Short-term recall: 2 users forgot 1 password and 1 forgot 2 passwords.
- Long-term recall: 4 users forgot 1 password.

For 5-restriction group,

- Short-term recall: 1 user forgot 1 password, 2 forgot 2 passwords, and 2 forgot all 3 passwords.
- Long-term recall: 3 users forgot 1 password, 3 forgot 2 passwords and 2 forgot all 3 passwords.

Discussion:

- The sentence generation method improved the security of passwords when additional restrictions were imposed that required inclusion of a special character and digit.

- However, the additional restrictions resulted in a cost in the memorability of passwords for both short-term and long-term recall.

- Poorer performance in recalling passwords with the additional restrictions was due to errors in:

1. Recall of where the special character and digit were placed within the sentence (4.5%)
2. Recall of the exact wording of the sentence (37.5%)
3. Recall of the special character and/ or digit (25.5%)
4. Recall of both the sentence and the special character and/ or the digit (13.5%)
5. Use of a password for a different account (19.5%)

- Failure to remember the sentences could have been due to the participants remembering the gist of the sentence instead of the exact phrasing.

- Interference occurred between passwords for different accounts.

Future Work:

Based on the analysis of errors, further studies could be done to identify:

- Methods that can be used to help users remember the exact phrasing of the sentence.
- Mnemonic techniques for remembering the digit and/ or special character used in the sentence.
- Mnemonic techniques for relating sentences to account names.