Effect of Two-Factor Authentication On Users' Trust in Their Passwords

Marley Jenkins, Malik Smith, and Brandon Bradley Winthrop University
Dr. Andrew Besmer Faculty Mentor

Introduction

.

This project focuses on examining the relationship between Two-Factor Authentication (2FA) and the strength of passwords. We are investigating users' trust towards the security of their passwords, depending on whether they implemented 2FA.

Objectives

The objective of this research study is to answer the following research question:

Does Two-Factor Authentication (2FA) have an effect on the strength of user's passwords?

Limitations

- Small Sample Size
- Only Winthrop University students
- Potentially skewed data due to possibility of people retaking treatment survey
- No risks involved for participants therefore password scores might be arbitrary
- Small Treatment Group

Method

Each study was sent out via Winthrop's Student ListServ, Discord Servers and Snapchat

No passwords were collected to ensure the privacy and security of the participants.

Control Group

- Instructed to create faux social media account.
- Created a fake username and think of a password.
- Answered survey question based on password to determine score and their demographic.

Treatment Group

- Instructed to create faux social media account with Two- Factor Authentication
- Created a fake username and think of a password.
- Answered survey question based on password to determine score and their demographic.

Collected Data

- Control Group:
  - 32 Respondents
  - Age: 18-28
  - Classification: Undergrad-Graduate Students
  - Major: Diverse (Non-Computing-Computing)
- Treatment Group
  - 22 Respondents
  - Age: 19-38
  - Classification: Undergrad-Graduate
  - Major: Diverse (Non-Computing-Computing)

Findings

- When applying the Mann-Whitney U test to our data and comparing the individual password score for the participants between the Control Group (Figure 2) and the Treatment Group (Figure 1) , we found that there was no significant difference at a p value < 0.05.
- The Z-score was -0.46371 and the p-value was .64552. This indicates that the samples of both the Control Group and the Treatment group failed to reject the null hypothesis.

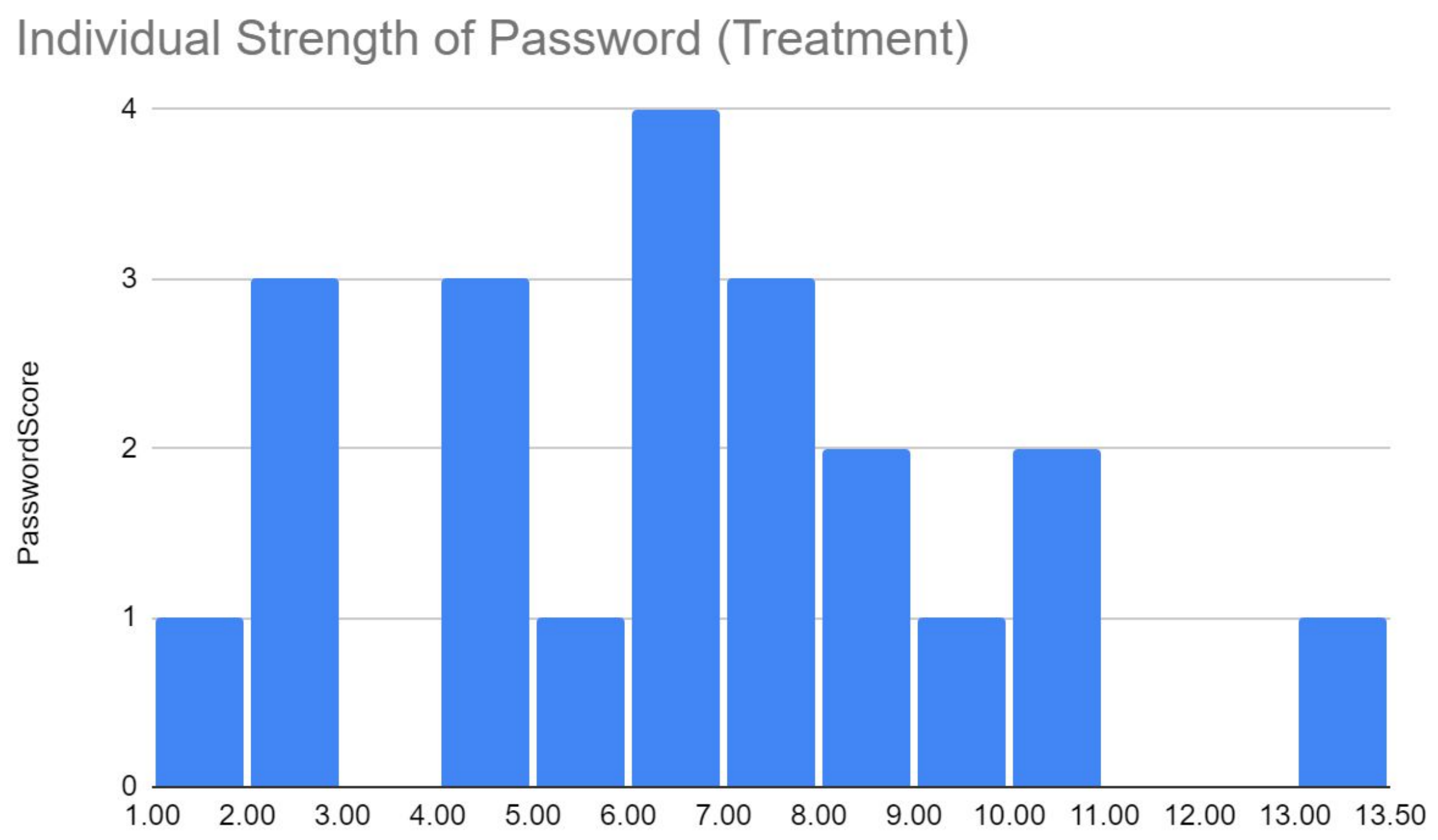

Figure 1: *Histogram displaying the results of the number of Individual Strength of Passwords For the Treatment Group.*

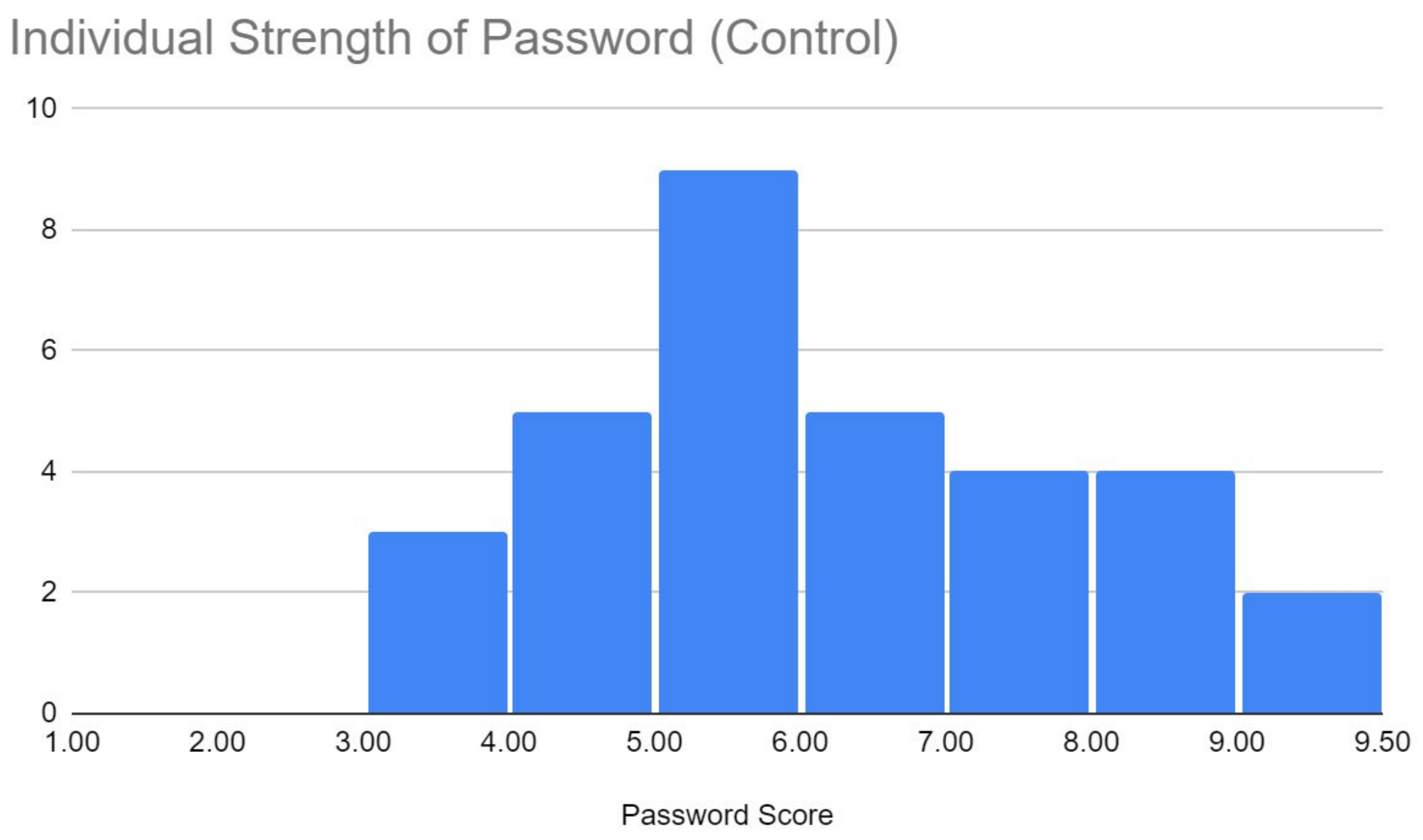

Figure 2: *Histogram displaying the results of the number of Individual Strength of Passwords For the Control Group.*

Conclusion

Our study failed to reject the null hypothesis so we could not detect differences between the control and treatment groups. Before attempting to draw conclusions with the original study we replicated. We believe that this study should be replicated again with the following improvements:

- Using a bigger sample size and spread out the study over a larger population with a more diverse demographic.
- Provide a greater incentive/motivation.
- In our study as well as the study we replicated there was not a sufficient incentive offered to make participants more likely to actively try to comply.
- Determine a better way of determining password strength. password strength doesn't factor in certain nuances between passwords which could have helped make our data more accurate, diverse, and complete.

Future Work

- Improving the measurement instrument by replicating our study with the measurement tool of the original paper called entropy.
- Run a study measuring the current attitude of people setting passwords. See how that impacts password strength.

References

Wimberly, Hugh & Liebrock, Lorie. (2011). *Using Fingerprint Authentication to Reduce System Security: An Empirical Study*, 32-46.