Towards Creating a Social Authentication System

Michelle Ling
Advised by: Cori Faklaris
Human-Computer Interaction Institute, Carnegie Mellon University, Pittsburgh, PA 15213

I. Background

Account Sharing Habits

According to a study conducted by SurveyMonkey, more than one-third of workers in the U.S. share accounts with their coworkers [1]. The study also found that nearly one-fourth of people reuse passwords between multiple work accounts. However, more than 80% of hacking incidents can be attributed to stolen or weak passwords. With the average American worker managing 27 online accounts [2], maintaining an efficient and secure workplace account becomes quite burdensome.

Benefits of Account Sharing

- Can easily manage individuals' access to specific files and information
- Can circumvent possibly lengthy account verification and approval processes
- Centralized location for files; easily accessible
- Can be less costly than individual account subscriptions

Disadvantages of Account Sharing

- Passwords are tedious to remember; security becomes compromised when members write down passwords or share them with other workers/accounts
- One individual can lock out everyone's access to the account
- If passwords are required to be changed every so often, updating all the members and having remember new passwords can be difficult
- If passwords are not required to be changed, former members can still access the account even though they have left the group

Types of Authentication Methods

There are three main categories that most authentication mechanisms fall under:

- Something we have (e.g. key card, phone applications)
  - Advantages: easy for two-factor authentication, no additional information
  - Disadvantages: can be easily stolen or lost
- Something we know (e.g. passwords, security questions, PIN numbers)
  - Advantages: can be very difficult to break
  - Disadvantages: sharing across multiple online accounts, can be stolen if written down, can forget if difficult to remember or easily guessed if easy to remember or short in length
- Something we are (e.g. fingerprint scan, facial recognition, voice recognition)
  - Advantages: unique, cannot be forgotten or stolen
  - Disadvantages: sensitivity affects accuracy, no real standard, can be difficult to implement

II. Objectives

To create a social authentication system that

- Is more accessible and efficient for individual users
  - Cannot be locked out due to their coworkers
- Develops workgroup culture and accountability
- Does not require the use of any additional/extraneous information
- Utilizes the face-to-face interactions between coworkers
- Is dynamic; works independently of the members in the group

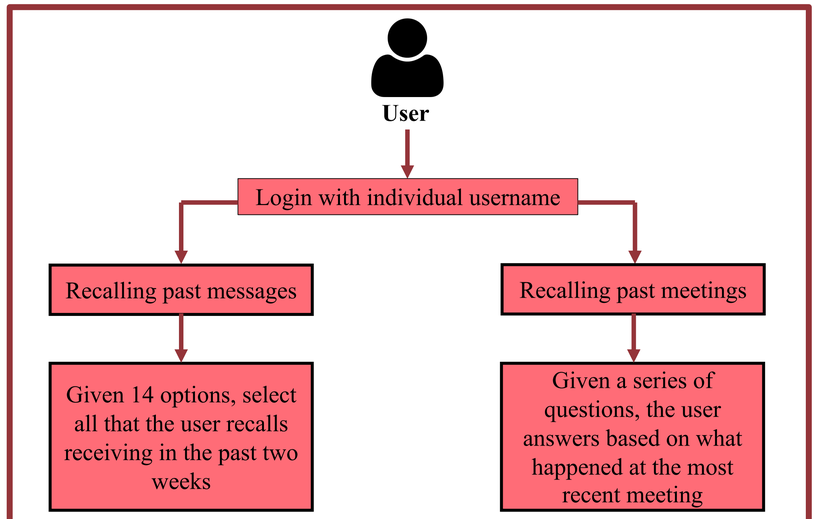

Figure 1. Login process that demonstrates the dual-component system

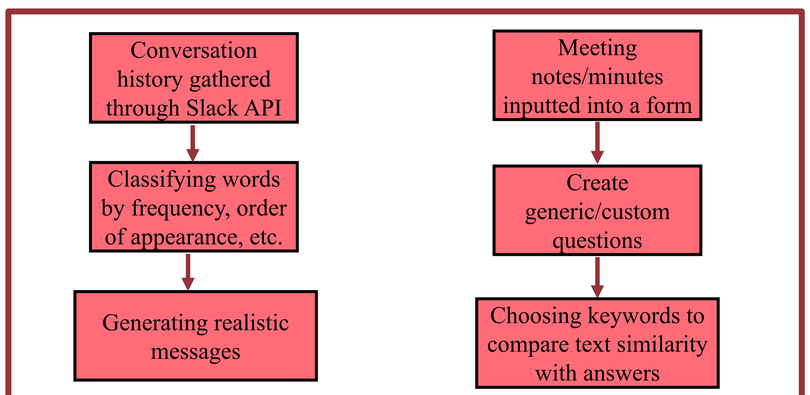

Figure 2. Data generation process for each component of the system

III. System

Design

As shown in Figure 1, the system is split into two components that appeal to different shared interactions between members in a work group.

- Notes from meetings
  - Free-response questions based on the contents of the meeting notes reflect the security of traditional passwords
- Past conversation messages
  - Select-all-that-apply questions with a mix of 14 real and generated messages mimics the security of a 4-digit PIN number

Use cases

- In lieu of two factor authentication as an alternate/backup authorization method for shared accounts
- Improve accountability for groups who struggle to take meeting notes and build work group culture through emphasizing a strong sense of shared knowledge

IV. Methods

Conversation history retrieval	- **Slack API** to create an app that retrieves recent messages in a Slack channel
Sentence generation	- **Pandas** and **NumPy** libraries in **Python** to classify words and generate messages based on specific existing messages within a group

Meeting notes webform & Login interface	- **HTML** and **JavaScript** to create the webform
	- **Node.js** to integrate components
	  - Collect and modify data
	  - Run the login process

V. Future Work

- Develop a more sophisticated sentence generation algorithm
  - Classify messages based on sensitivity of content so that private information is not revealed to users
  - Compare frequency of words between channels to find group-specific jargon
- Implement a more accurate answer verification system using fuzzy logic and keywords
- Create a secure data storage system

VI. References

1. Williams. 2019. The dangers of password sharing at work. (March 2019). Retrieved May 3, 2020 from https://www.techradar.com/news/the-dangers-of-password-sharing-at-work
2. Tawny S. 2019. Google Says 66% of Americans Still Do This 1 Thing That Puts Their Personal Information at a Huge Risk. Here's How Google Wants to Help. (November 2019). Retrieved May 3, 2020 from https://theharrispoll.com/google-says-66-of-americans-still-do-this-1-thing-that-puts-their-personal-information-at-a-huge-risk-heres-how-google-wants-to-help/
3. Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. 2019. Normal and Easy: Account Sharing Practices in the Workplace. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 83 (November 2019), 25 pages. https://doi.org/10.1145/33591855.

VII. Acknowledgements

This project is part of the HCII Social Cybersecurity project, sponsored by the U.S. National Science Foundation under grant no. CNS-1704087.
Special thanks to my advisor Cori Faklaris, Laura Dabbish, Jason Hong, Anna Cai, and Serena Wang.