CNT 5410: Computer and Network Security

Final Project Report: Beyond the Key Enhancing Password Security Through Comprehensive Research and Practical Insights

Nishant Agrawal
(Point of Contact)
agrawal.nishant@ufl.edu

Pavan Kumar Appikatla
pappikatla@ufl.edu

Sreekar Reddy Nathi
sreekarreddnathi@ufl.edu

Gopi Amarnath Reddy Bekkem
bekkem.g@ufl.edu

Kushi Vardhan Reddy Pasham
kushivardhpasham@ufl.edu

Gangula Vivek Reddy
gangula.v@ufl.edu

December 9, 2023

1 Introduction

In today's world it's a critical concern that passwords can easily be hacked. As the technology is advancing, the hackers are also advancing so it is very important to make sure that security through passwords is strong and secure. Many databases are getting compromised on a day to day basis, password security can be a matter of concern in the coming future. Through this paper we want to get a better understanding of the security of the passwords.Our research includes analysis of about 15 research papers that discuss password security and the challenges revolving around it. We are not only looking at the technical perspective but also how the users think while they create the passwords through a survey about their perception of the password as a security feature and whether there is a need for a new authentication mechanism. We want to figure out the problems and suggest good ways to make digital spaces safer for people and organizations.

2 Background & Related Work

In today's digital world, where everyone is mostly involved in online work or online tasks, keeping our personal and private information safe is really important. Though a number of authentication mechanisms have come into picture, passwords still stand out as one of the largest authentication mechanisms. Passwords are used to gain access to most important user data like emails, social media, and bank accounts. But the burning problem is that hackers on the internet are constantly trying to guess/crack these passwords. Passwords can be guessed easily by these people using different techniques like brute force attack or through fake emails or websites (phishing). There are even attacks like dictionary attacks or rainbow table attacks. Because of these risks, there has been a constant study going on to make these passwords safe from these hackers. The passwords need to be more complex to stay resistant from guessing. But remembering many complex passwords is difficult for most people, and they prefer to have simple easy-to-guess passwords which causes serious threats when it comes to security. In recent times, new methods have been developed to make passwords more secure. Some websites use two-factor authentication. There are also password managers, which are like digital vaults for storing passwords. They create and store strong passwords for people.[2]

In summary, while passwords are still crucial for our online security, it's important to be aware of their limi- tations. Hence a continuous study has been going on in this field of password security, the ways to resist hackers from breaking the passwords, various user behavioral patterns in creating passwords, AI tools to study passwords and their strengths.

We have gone through extensive research made in the field of password security and have gained valuable insights to some of the crucial aspects to maintain better password security. We have discussed them briefly in the next sections.

3 Approach: Dataset(s) & Technique(s)

We have completed the review of approximately 15 research papers and many online articles about online attacks and breaches, thoroughly analyzing and delving into the findings and propositions presented in each paper. Our focus has been on understanding the nuances of password security, and through a holistic examination of these papers, we have identified previously unexplored areas in the realm of password protection.

Our approach involved a meticulous study of the propositions put forth by the authors. We dedicated considerable effort to comprehending the finer details of how passwords are safeguarded. The goal was not merely a cursory glance at the research papers; rather, our intent was to gain a deep understanding of the content and unearth novel insights that may not have been discussed in the broader landscape of password security.

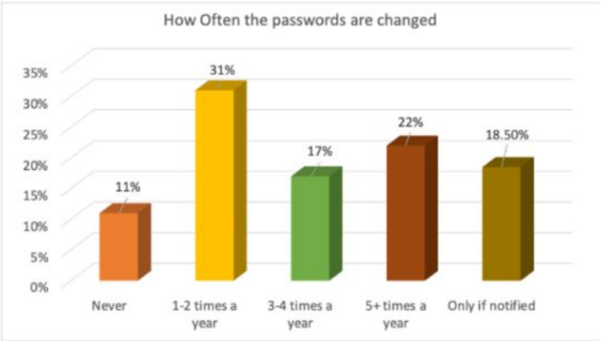
Our ultimate objective is to contribute to the broader understanding of password security. By exploring new ideas and venturing into areas that have received limited attention in previous studies, we aim to advance knowledge in this field. Our findings are poised to assist others in enhancing their comprehension of password security and, in turn, contribute to the ongoing discourse on this critical aspect of cybersecurity.

3.1 User Survey

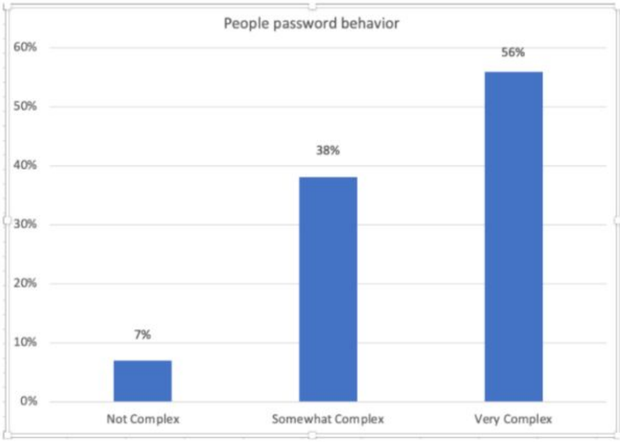
3.1.1 As part of our study about passwords we have used "Uncovering Password Habits: Are Users' Password Security Habits Improving?" survey by Nate Lord[1] (Infographic) and these are the observations that we found:

The survey, conducted on 1,000 internet users, provides insights into the evolving landscape of password security habits. Five years ago, 89% felt secure with their password habits, yet 61% admitted to reusing passwords across multiple websites. Over the years, certain habits have improved, but challenges persist.

Password overload is a widespread issue, with 70% of respondents managing more than 10 password-protected accounts. The average email address in the U.S. is linked to 130 accounts, highlighting the complexity users facein managing passwords. Despite awareness of risks, 49% of respondents still reuse passwords, though often for less sensitive accounts. Difficulty remembering passwords leads to risky behaviors, such as writing them down on paper (39%) or keeping them in insecure files (17%).



On a positive note, 70% of users change their passwords at least once a year, with 40% doing so three times or more annually. Users are also creating complex passwords, with 56% incorporating a mix of uppercase, lowercase,numbers, and special characters.



The survey delves into generational differences, revealing that younger age groups tend to create more complex passwords. Additionally, 65% of users prioritize security over convenience when crafting passwords.

Encouragingly, 48% of respondents use two-factor authentication, bolstering their account security. The survey concludes with a set of best practices, emphasizing regular password updates, avoiding reuse, prioritizing passphrases, leveraging two-factor authentication, and employing secure password management.

In conclusion, the survey indicates a mixed landscape of evolving password habits. While improvements are evident, challenges persist, emphasizing the need for continued education on robust password hygiene practices

4 Case Studies

4.1 Reddit Breach

In February 2023, Reddit fell victim to a sophisticated and highly-targeted phishing attack[1], marking a significant security breach in the company's history. This type of attack involved sending plausible-sounding prompts to Reddit employees, directing them to a counterfeit website that mimicked Reddit's

[1] Reddit breached:https://www.malwarebytes.com/blog/news/2023/02/reddit-systems-compromised-by-phish-attack-heres-wha

intranet portal. The goal was to deceive employees into entering their login credentials and two-factor authentication (2FA) tokens. Unfortunately, the attackers were successful in this endeavor, compromising the credentials of at least one employee. This breach allowed the attackers, identified as the BlackCat (ALPHV) ransomware gang, to gain unauthorized access to Reddit's internal systems.

The extent of the data breach was considerable, with the attackers claiming to have stolen around 80GB of compressed data from Reddit. The stolen data primarily included internal documents, source code, employee data, and limited data about Reddit's advertisers[2]. Following the attack, Reddit took several proactive steps to mitigate the damage and prevent future incidents. These measures included promptly removing the infiltrator's access upon discovery, commencing an internal investigation, and reinforcing their security protocols. Additionally, Reddit was transparent in its communication with users, hosting an "Ask Me Anything" (AMA) session to address concerns and advise users on enhancing their account security, notably recommending the setup of two-factor authentication

4.2 Sony Password Breach

In 2023, Sony Interactive Entertainment experienced two significant data breaches. The first breach was a result of a zero-day vulnerability in the MOVEit Transfer platform, specifically CVE-2023-34362. This critical-severity SQL injection flaw allowed for remote code execution and was exploited by the Clop ransomware gang, known for carrying out large-scale cyber attacks. The breach led to the compromise of personal information of approximately 6,800 individuals, primarily current and former employees and their family members in the U.S. The types of data compromised in this breach included sensitive personal information, although the specifics were not publicly detailed.

[3] In response to these incidents, Sony took several critical steps to mitigate the damage and prevent future attacks. They immediately shut down the affected platform upon discovering the breach, remediated the vulnerability, and launched an investigation with the help of external cybersecurity experts. Additionally, Sony notified law enforcement agencies about the breach. To support those affected by the breach, Sony offered credit monitoring and identity restoration services through Equifax, providing individuals with unique codes for access to these services until February 2024. These actions reflect Sony's commitment to addressing cybersecurity challenges and protecting the interests of its stakeholders[4]

4.3 Proposal

4.3.1 Problem Statement / Existing scenario:

In the current landscape, most applications operate with a uniform password policy for all users. However, through our observations, we've identified a vulnerability in this approach, particularly affecting users who may not be aware of potential password-related risks.

A universal password policy may not cater to the diverse awareness levels of users; some individuals are well-versed in password-related issues, while others lack awareness. It is crucial for websites to consider and address the needs of users with varying levels of knowledge, especially those who may be less informed about password security.

To address this, we propose the introduction of a new metric, the "User Safety Score," ranging from

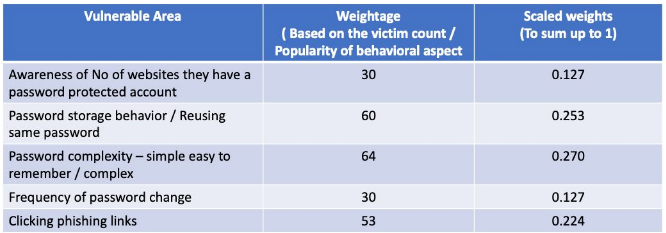
[2] Reddit Suffers Security Breach Exposing Internal Documents and Source Code:https://thehackernews.com/2023/02/reddit-suffers-security-breach-exposing.html

[3] Sony Confirms Data Breach Impacting Thousands in the U.S Code:https://www.bleepingcomputer.com/news/security/sony-confirms-data-breach-impacting-thousands-in-the-us/

[4] Sony Data Breach Confirmed Code:https://dataconomy.com/2023/10/04/sony-data-breach-2023-playstation-leak/

a minimum of 0.25 to a maximum of 1. This score takes into account various behavioral aspects of users to determine their level of vulnerability.

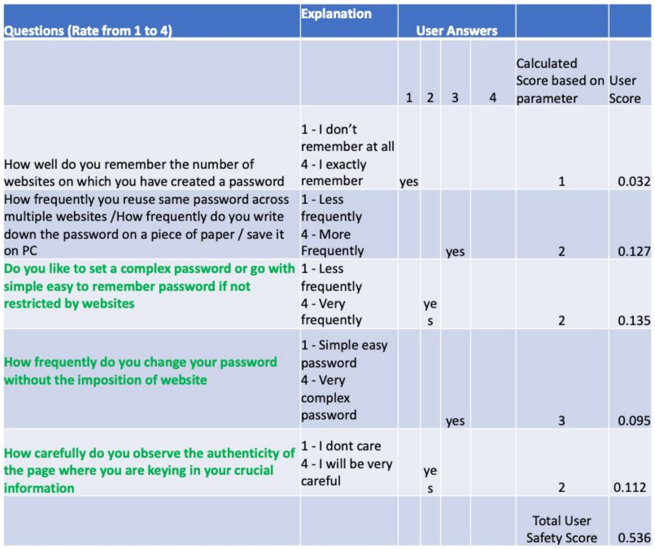
We have identified particular areas of vulnerability and allocated weights according to the number of victims and the prevalence of behavioral factors. These areas encompass consciousness regarding the quantity of password-protected accounts, patterns of password storage, password complexity, frequency of password changes, and susceptibility to clicking on phishing links.



Vulnerable Area	Weightage (Based on the victim count / Popularity of behavioral aspect	Scaled weights (To sum up to 1)
Awareness of No of websites they have a password protected account	30	0.127
Password storage behavior / Reusing same password	60	0.253
Password complexity – simple easy to remember / complex	64	0.270
Frequency of password change	30	0.127
Clicking phishing links	53	0.224

To compute the User Safety Score, individual users need to respond to a series of questions (at the initial stage of signup), assigning scores from 1 to 4. These questions gauge their understanding of password-related behaviors, encompassing aspects such as recalling the number of websites with password-protected accounts, the practice of password reuse, preferences for password complexity, the frequency of password changes, and caution regarding phishing links.

Users will be categorized based on their User Safety Score, calculated through both a questionnaire and continuous monitoring during website usage.

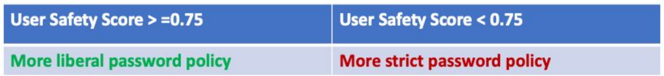


Questions (Rate from 1 to 4)	Explanation	User Answers					
		1	2	3	4	Calculated Score based on parameter	User Score
How well do you remember the number of websites on which you have created a password	1 - I don't remember at all 4 - I exactly remember	yes				1	0.032
How frequently you reuse same password across multiple websites /How frequently do you write down the password on a piece of paper / save it on PC	1 - Less frequently 4 - More Frequently			yes		2	0.127
Do you like to set a complex password or go with simple easy to remember password if not restricted by websites	1 - Less frequently 4 - Very frequently		yes			2	0.135
How frequently do you change your password without the imposition of website	1 - Simple easy password 4 - Very complex password			yes		3	0.095
How carefully do you observe the authenticity of the page where you are keying in your crucial information	1 - I dont care 4 - I will be very careful		yes			2	0.112
						Total User Safety Score	0.536

A green category indicates that the user's responses can be validated during application usage, while a black category relies solely on user answers.

We can use either Min(QuestionnairebasedUserSafetyScore, DynamicUserSafetyScore) for a stringent policy making or

Avg(QuestionnairebasedUserSafetyScore, DynamicUserSafetyScore) for a lenient policy making.



User Safety Score > =0.75	User Safety Score < 0.75
More liberal password policy	More strict password policy

We've set a threshold for the User Safety Score at 0.75. This threshold is reached when a user consistently scores 3 out of 4 for each question. This metric becomes particularly useful for banking and other websites involving monetary transactions, offering a safer application environment for customers.

4.3.2 Future Work

Furthermore, this approach can be extended by implementing real-time user behavioral pattern analysis, allowing us to adapt security measures dynamically based on how users interact with anonymous or potential phishing links.

5 Results

5.1 Results from our Study

5.1.1 Password Vulnerabilities

Identification of common vulnerabilities in passwords, such as susceptibility to brute force attacks, phishing, and dictionary attacks.

Analysis of how hackers exploit these vulnerabilities to compromise user accounts and sensitive information.

5.1.2 User Perspectives

Survey results on user perceptions of password security.

Insights into user behaviors and preferences when creating passwords.

Understanding the trade-off between security and convenience in password creation.

5.1.3 Authentication Mechanisms

Evaluation of alternative authentication methods beyond traditional passwords.

Examination of the effectiveness of two-factor authentication and password managers.

5.1.4 Technological Advancements

Overview of AI tools and technologies used in enhancing password security.

Identification of emerging trends in password protection technologies.

5.2 Results of our new methodology

Anticipated results include a notable reduction in password-related vulnerabilities, fostering a heightened level of trust among users. The dynamic adaptation to user behavior ensures a more resilient security framework, stringent password policies instilling confidence in the safety of online interactions. This user centric custom password policy might make the user more vigilant and creates an opportunity to make his password safe.

6 Conclusions

In conclusion, our project on password security raised several issues with standard password policies, particularly in light of the increasing number of data breaches and skilled hackers in the world. We must consider alternatives to the conventional methods for protecting our data.

No individual technology can ensure the complete safety of a person's password from being compromised.

It is the responsibility of individuals to stay informed about potential issues and remain vigilant.

We've discovered a new approach that can be employed by organizations to safeguard individuals' password security.

6.1

References

[1] Nate Lord. Uncovering password habits: Are users' password security habits improving? (infographic). *Digital Guardian's Blog*, 2020.

[2] A Harshel Srivatsava Sravan Duggi Venkat Jonnalagadda Sony Kuriakose, G Krishna Teja. Machine learning based password strength analysis. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 11(8):1–4, 2022.