COMPUTER AND NETWORK SECURITY

Beyond the Key Enhancing Password Security Through Comprehensive Research and Practical Insights

Group - 11

Nishant Agrawal

Sreekar Reddy Nathi

Kushi Vardhan Reddy Pasham

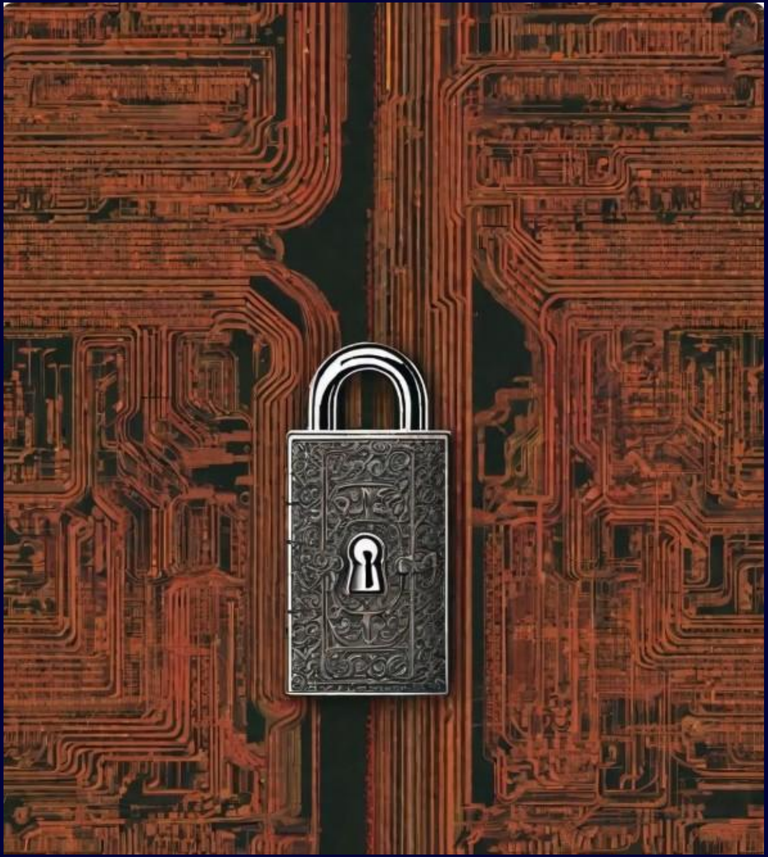
Pavan Kumar Appikatla

Gopi Amarnath Reddy Bekkem

Gangula Vivek Reddy

PROBLEM DEFINITION

- Emphasis on the increasing incidents of database compromises and potential future concerns.
- Discuss the advancement of hacking techniques paralleling technological development.
- Need for a robust authentication mechanism beyond traditional password systems.

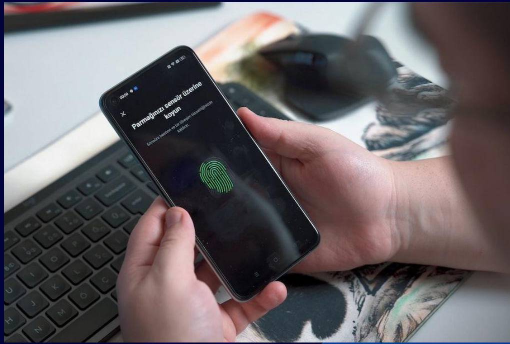


Introduction

- Exploring the critical concern of easily hackable passwords in the advancing technological landscape.
- Objective: To gain a deeper understanding of password security through comprehensive research.
- Importance of strengthening password security in protecting personal and organizational data.

Literature Survey

- Machine Learning and Artificial Intelligence (AI) in Password Security
- Multi Factor Authentication (MFA) Systems
- Biometric Passwords
- Password Managers
- User Education and Human Factors

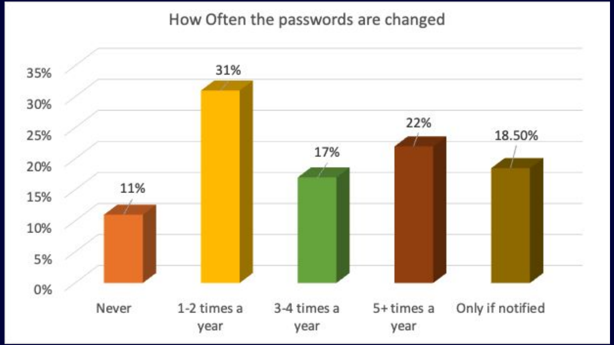


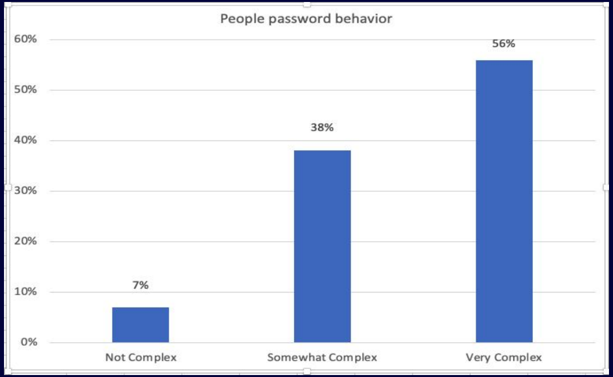
Results/ Analysis

- User behavioral analysis on reluctance to use Online Password Managers
- User education and human behavioral patterns
- Even multi-factor authentication is not safe!!

Insights from "Uncovering Password Habits" Survey

- Evolving Password Habits: 89% felt secure in their password habits five years ago, but 61% admitted to reusing passwords across sites.
- Password Management Challenge: 70% manage over 10 password-protected accounts, with the average U.S. email linked to 130 accounts.
- Improvements and Risks: Despite 49% reusing passwords, 70% change their passwords yearly, with 56% using complex character combinations.
- Adoption of Enhanced Security Measures: 48% use two-factor authentication, showing a trend towards prioritizing security over convenience.





Reddit Breach

- Reddit experienced a sophisticated phishing attack in February 2023.
- The BlackCat (ALPHV) ransomware group claimed responsibility for the Reddit breach.
- Attackers exfiltrated approximately 80GB of data, including internal documents and source code.
- Reddit responded with an internal investigation, notifications to affected parties, emphasizing cybersecurity awareness among employees, and recommending two-factor authentication (2FA) for users to enhance security.

Sony Password Breach

- The 2023 data breach at Sony Interactive Entertainment resulted from a critical-severity SQL injection flaw (CVE-2023-34362), allowing for remote code execution.
- The breach was orchestrated by the Clop ransomware gang, known for large-scale cyberattacks, exploiting the zero-day vulnerability in the MOVEit Transfer platform.
- Approximately 6,800 individuals were affected, primarily current and former employees and their family members in the U.S.
- Sensitive personal information was compromised, with specific details undisclosed.
- Sony responded by swiftly shutting down the platform, fixing the vulnerability, involving external experts, notifying law enforcement, and offering credit monitoring and identity restoration services through Equifax until February 2024.

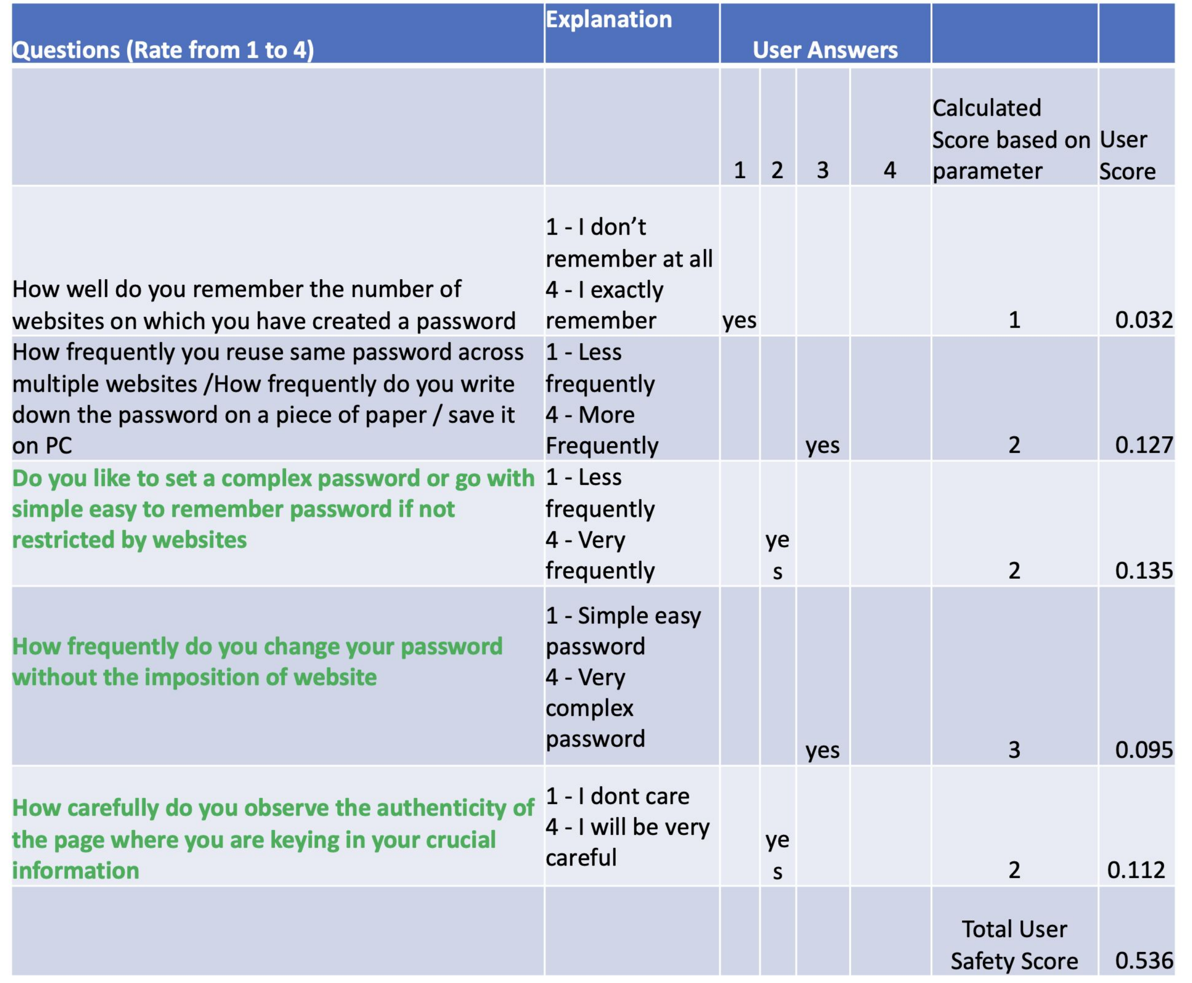
Dat

Dynamic User centric password policy based on “User Safety Score”

- Majority of the applications in the present world are working on based on single password policy for all the users
- We observed a kind of vulnerability in this model
- Especially users who are not aware of potential issues with password vulnerabilities
- Considering the behavioral aspects of users, we may need to have user centric password policy.
- For this, we have come up with a new metric called “**User Safety Score**” (Min 0.25, Max 1)

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

- User will be categorized based on the “User safety score” calculated in two different ways.
- 1. Based on the questionnaire
- 2. Based on the continuous monitoring system while the usage of the website
- **Green** – Can be validated while application usage
- **Black** – Will be relied on users' answers



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

- We have defined a threshold for this ”User safety score” which is 0.75.
- This threshold is arrived when the user gets an average score of 3 out of 4 for each question.

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

- Will be extremely helpful for banking websites / other websites where monetary transactions are involved.
- Till now, we haven’t seen such websites concentrating on this to make their application usage safer place for customers.

Pseudo Code

```
UserSafetyScore(Responses{‘question’: ‘response’}):
UserSafetyScore = 0
For question, response in Responses:
    Switch(question):
        ‘How well do you remember the number of websites on which you have created a password’:
            UserSafetyScore + = Response * 0.127 / 4

        ‘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’:
            UserSafetyScore + = (5 – Response) * 0.253 / 4

        ‘How frequently do you change your password without the imposition of website’:
            UserSafetyScore + = Response * 0.127 / 4

        ‘Do you like to set a complex password or go with simple easy to remember password if not restricted by websites’:
            UserSafetyScore + = Response * 0.270 / 4

        ‘How carefully do you observe the authenticity of the page where you are keying in your crucial information’:
            UserSafetyScore + = Response * 0.224 / 4

Return UserSafetyScore
```

Data Breach

Future Work

- This can be extended further by dynamically studying the user behavioural patterns to anonymous links etc.

Conclusion

Thank You