CYBER SECURITY

PASSWORD STRENGTH

Presented By:
S.Soundharya
Salem college of Engineering and Technology
Computer science and Engineering

OUTLINE

- Problem Statement
- The Frontline of Defense
- The Enemy at the Gate
- Forging Your Shield
- Beyond the Wall
- Building a Secure Future
- Conclusion
- References

PROBLEM STATEMENT

Design and implement a password strength checker application that evaluates the strength of user-generated passwords based on various criteria such as length, complexity, and uniqueness. The application should provide feedback to users on the strength of their passwords and suggest improvements if necessary. Additionally, it should incorporate measures to prevent common security vulnerabilities such as dictionary attacks and brute force attacks. The goal is to ensure that users create strong and secure passwords to protect their accounts from unauthorized access

THE FRONTLINE OF DEFENSE: WHY STRONG PASSWORDS MATTER

In today's digital world, our online accounts hold a treasure trove of personal information, from financial records to private messages. These accounts are the gates to our digital lives, and strong passwords are the key to keeping them secure. Just like a knight guarding a castle gate, a strong password acts as the first line of defense against unauthorized access. In this presentation, we'll explore the importance of password strength, common password pitfalls, and best practices for creating unbreakable passwords.

THE ENEMY AT THE GATE: COMMON PASSWORD WEAKNESSES

- Simple Dictionary Words: Attackers can easily guess passwords that are common words found in the dictionary.
- Personal Information: Birthdays, pet names, addresses – these are easily obtainable details that should never be used in passwords.
- Reused Passwords: Using the same password for multiple accounts creates a domino effect – if one account is compromised, they all are.
- Short Passwords: The shorter the password, the easier it is to crack. Aim for at least 12 characters.

FORGING YOUR SHIELD:
THE ELEMENTS OF A STRONG PASSWORD

- Length is Key: Aim for passwords with at least 12 characters, the more the better.
- Complexity is King: Include a mix of uppercase and lowercase letters, numbers, and special symbols.
- Uniqueness is Power: Create unique passwords for each account, avoiding any reuse.
- Avoid the Obvious: Don’t use keyboard patterns (e.g., 12345) or simple substitutions (e.g., P@ssw0rd).

BEYOND THE WALL:
ADDITIONAL SECURITY MEASURES

- Two-Factor Authentication (2FA): Adds an extra layer of security by requiring a • second verification code in addition to your password.
- Password Managers: Securely store and manage strong, unique passwords for all your accounts.
- Regular Password Updates: Change your passwords periodically, especially after any potential security breaches.

BUILDING A SECURE FUTURE:
REMEMBER THE POWER OF STRONG PASSWORDS

Strong passwords are the cornerstone of cybersecurity.

By following the best practices outlined here, you can significantly improve your online security posture.

Remember, a strong password is your digital shield, protecting your valuable information from unauthorized access.

CONCLUSION

This work describes the machine learning approach for determining the strength of the password. Support Vector Machine, a supervised pattern classification technique has been applied for training the password strength analysis model. Features are extracted from the set of 10,000 passwords of different categories to facilitate training and implementation.

REFERENCES

Cryptography and Network Security: Principles and Practice” by William Stallings – While not solely focused on password strength, this book provides a thorough overview of cryptographic techniques and network security principles, which are essential for understanding the foundations of secure password management.

THANK YOU

edunet
foundation