PREDICTING PASSWORD STRENGTH USING SUPERVISED MACHINE LEARNING TECHNIQUES

TEAM 14

GROUP MEMBERS

1. JASWANTH REDDY . L	21MAI0016
2. ANUSHA . P	21MAI0050
3. PUNITHA .G	21MAI0056
4. BATTA VENKATA SAIKUMAR	21MAI0063

LINK

https://drive.google.com/file/d/1_PxH5Hs3IpwQjS2j3ZjtbW2iLfIYFB42/view?usp=sharing

ABSTRACT

- Passwords are a vital component of system security. Despite the fact that there are many alternatives, passwords are still the most effective process of ensuring identity in many applications.
- They reflect an individual's identity for a system and give a simple, straightforward manner of preserving it.
- There are so many ways for an outsider with little technical knowledge or talent to acquire the passwords of legitimate users.
- Users are repeatedly informed that a strong password is vital these days to protect sensitive data.

ABSTRACT

- To ensure that these vulnerabilities are not exploited, organizations must be aware of the consequences that passwords bring and implement strong procedures for governing password generation and use.
- Classification based machine learning algorithm to classify the strength of passwords within predefined categories. Techniques like Decision tree classifier, Multilayer Perceptron, Naive Bayes Classifier, and Support Vector Machine can be used.
- The model with high accuracy can help to predict whether the password strength is strong or weak.

AIM

The Objective is to overcome vulnerabilities revolving around passwords and to safeguard the individual's identity in the system.

SCOPE

- Proper Authorization
- Reduce Fraud and Build Secure online Relationships
- Improved User Experience
- Increased Security
- Reduced administration overheads

INTRODUCTION

Passwords have become increasingly important in today's world. Passwords are required for a variety of tasks by a normal computer user, including logging into accounts, receiving e-mail from servers, transferring payments, shopping online, accessing applications, databases, networks, and web sites, and even reading the morning newspaper online.

Every day, the issue of choosing and utilizing strong passwords becomes more essential. The number and value of services supplied via computers and networks is rapidly increasing, and many of these services require passwords or other kinds of user authentication.

Users must use multiple passwords for different systems or services for a variety of reasons, including obvious security issues, making it more difficult to remember and protect one's password.

INTRODUCTION

Passwords are important not simply for logging in, but also in more advanced service-granting systems like Kerberos. Finally, passwords are required in authentication and encryption software, which is becoming increasingly important in many applications, to secure secret information that cannot be recalled by the user (e.g. private keys).

The average user prefers a password that is easy to remember and guess, rather than one that is strong. Data thieves, hackers, and other criminals are preying on those who aren't security savvy these days, and the threat is real and growing.

To guarantee that these weaknesses are not exploited, it is critical for companies to realize the risks that passwords face and to implement strong policies governing the generation and use of passwords.

MODULES

- FEATURE EXTRACTION
- ML MODELS
- TRAINING AND VALIDATION
- DEPLOYMENT USING DJANGO FRAMEWORK IN HEROKU CLOUD

FEATURE EXTRACTION

Feature selection plays an important role in improving classification effectiveness.

- Features include:
  - The Length of the password
  - Number of lowercase characters
  - Lowercase character weightage
  - Number of uppercase characters
  - Uppercase character weightage
  - Number of digits & digits weightage
  - Number of symbols & weightage of symbols
  - Number of middle number and symbols, Middle number/symbol weightage, Password contains characters only [case insensitive]

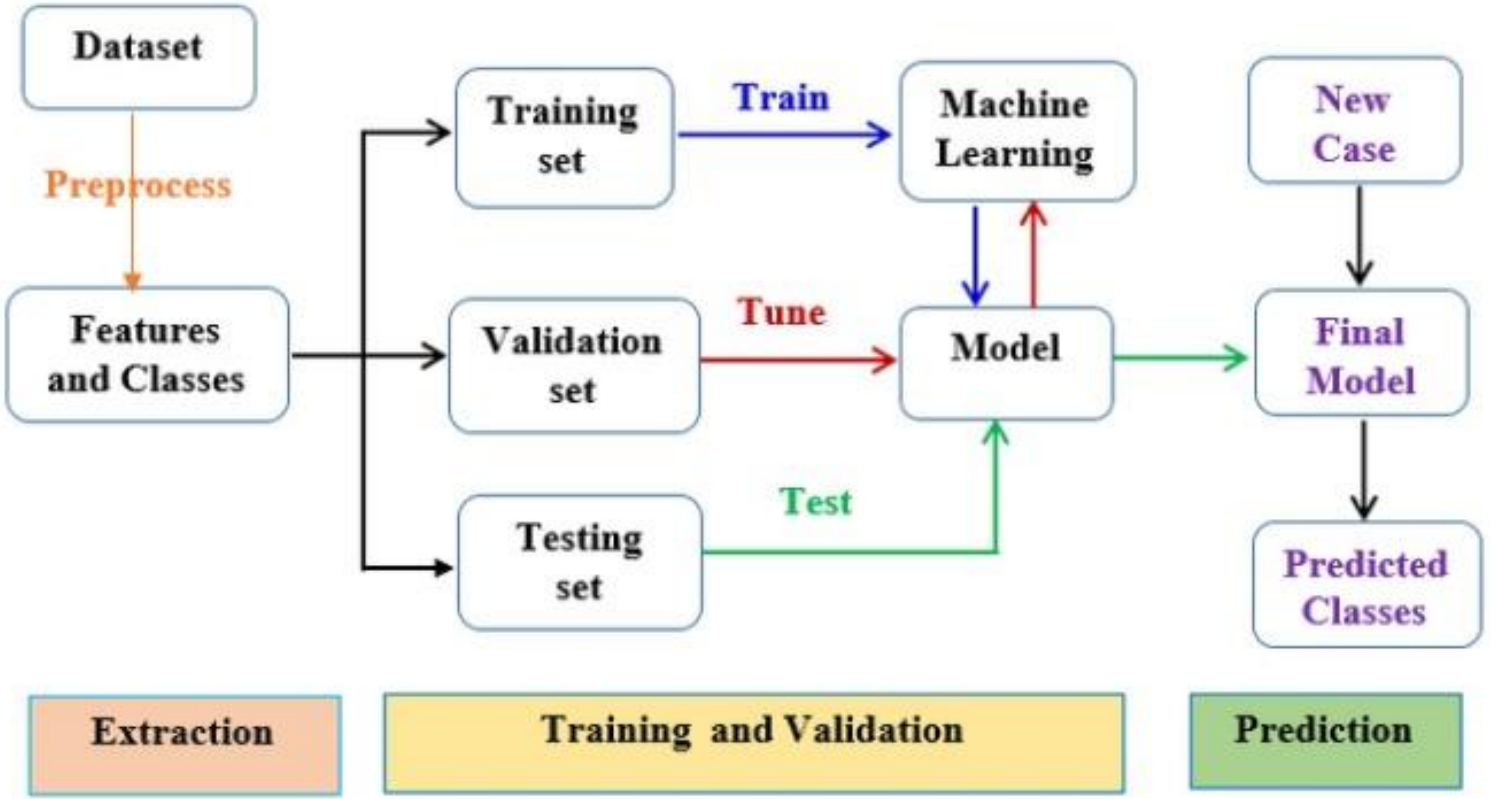
A weighting method was adopted for computing the strength of the password.The features that make the password strong were given more weightage and the features that weaken the password were given negative weightage.

ML MODULES

ML models are used to predict the vulnerability of passwords.

- SVM
- Naive Bayes
- MLP
- J48

WORKFLOW DIAGRAM



REFERENCES

[1] F.Bergadano, B.Crispo, G.Ruffo, "Proactive password checking with decision trees",Proc. of the 4th ACM conference on computer and communications security, Zurich, Switzerland, 1997, pp 67-77

[2] Giancarlo Ruffo, Francesco Bergadano, "EnFilter : A Password Enforcement and Filter Tool Based on Pattern Recognition Techniques", Springer Berlin / Heidelberg, 1611-3349 (Online), Volume 3617/2005

[3] Dell'amico, Matteo, Michiardi, Pietro and Roudier, Measuring Password Strength: An Empirical Analysis., Yves. Jul 20, 2009.

[4] Forget, Alain, Improving text passwords through persuasion, et al. s.l. : ACM, 2008. pp. 1--12.

[5] Narayanan, Arvind and Shmatikov, Vitaly. Fast dictionary attacks on passwords using time-space tradeoff. s.l. : ACM, 2005. pp. 364--372.

[6] B. Ur, P. G. Kelley, S. Komanduri, M. M. J. Lee, M. Mazurek, T. Passaro, R. Shay, T. Vidas and L. Bauer, "How does your password measure up? the effect of strength meters on password creation," in Proc. USENIX SEC 2012, 2012

REFERENCES

[7] D. Wang, Z. Zhang, J. Y. P. Wang and X. Huang, "Targeted online password guessing: an underestimated threat," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna Austria, 2016.

[8] D. Florencio, C. Herley and P. C. V. Oorschot, "Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts," in Proc. USENIX SEC 2014, 2014.

[9] J. Ma, W. Yang, M. Luo and N. L, "A study of probabilistic password models," in 2014 IEEE Symposium on Security and privacy, San Jose, CA, USA, 2014.

[10] M. K. L. Gong-Shen, Q. Wei-Dong and L. Jian-Hua, "Password vulnerability assessment and recovery based on rules mined from large-scale real data," Chinese Journal of Computers, vol. 39, no. 3, p. 454–467, 2016.

[11] D. Wang and P. Wang, "The emperor's new password creation policies," in in Proc. ESORICS 2015, 2015.

[12] M. Weir, S. Aggarwal, M. Collins and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in Proc. ACM CCS 2010, 2010.

THANK YOU !!