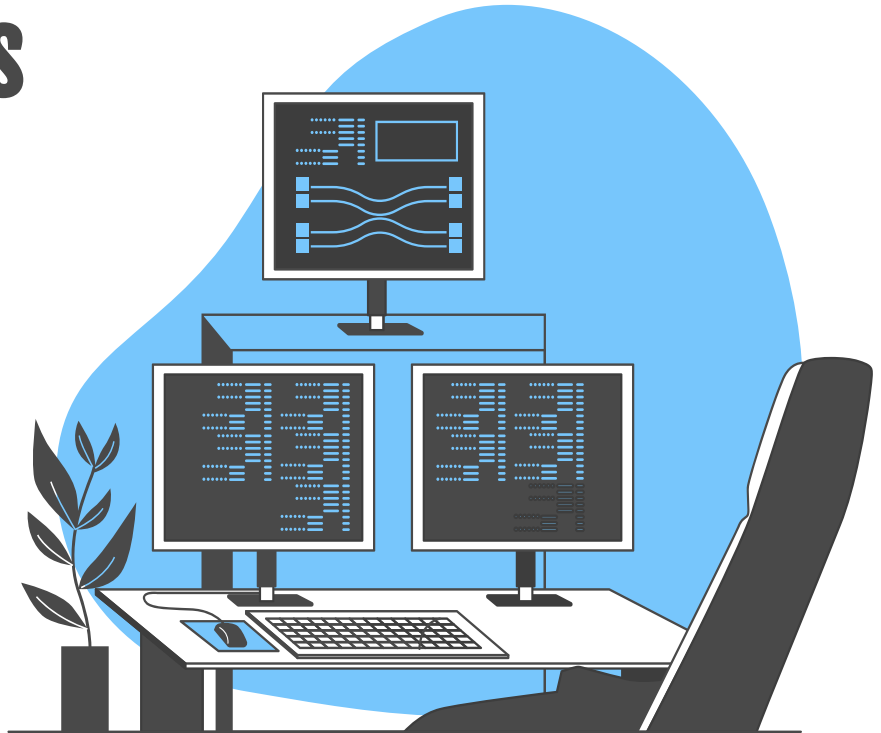
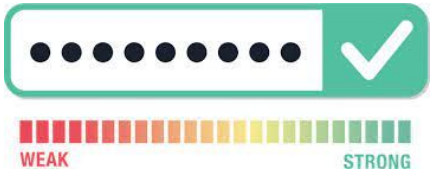
Improving the Systematic Generation of Secure and Memorable Passphrases by MASCARA

Kousshik Raj (17CS30022)
Supervisor:- Dr. Mainack Mondal



INTRODUCTION



Passwords Everywhere: Most common authentication secret, but difficult to manage.

Passphrases Alternative: Secure and memorable, used as authentication secrets or password generation contexts

MOTIVATION

1. **User Passphrases:** Chosen by user. Memorable, but predictable.
2. **Diceware:** Random words from wordlist. Secure, but low memorability.
3. **TemplateDice:** Improved Diceware, uses linguistic templates. Memorable, but not scalable, has security issues, etc.
4. **Mascara:** Constrained Markov generation, memorability and security tradeoff, but has issues and scope for improvement

CONTRIBUTIONS

- Improved guessability and memorability framework
- Analyzing the passphrases in use and their pros & cons
- Mascara: 10^4x speedup, better evaluation and results

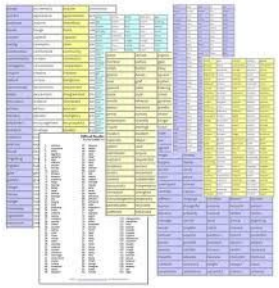
NOVELTY

Prior works on generating secure and memorable passwords using contextual cues, portmanteau, etc.

Prior works focus on behavioural patterns like login durations, frequency, etc. to estimate memorability. Uses user survey, no automated linguistic metric.

No earlier works on analyzing the systematic tradeoff between memorability and security of passphrases. MASCARA is one of the trailblazers in this area.

BACKGROUND: MASCARA

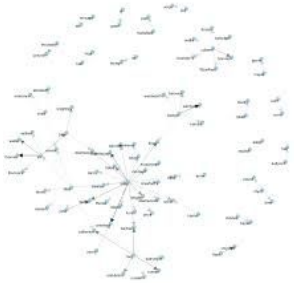


DATASET

Security

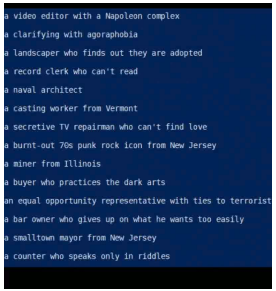
Memorability

FILTERING



BIGRAMS

WEIGHTED SAMPLING



INTERMEDIATE PASSPHRASE P_i

NEXT PHASE ($i = i + 1$)

MODIFICATIONS & RESULTS

Phrase Machine

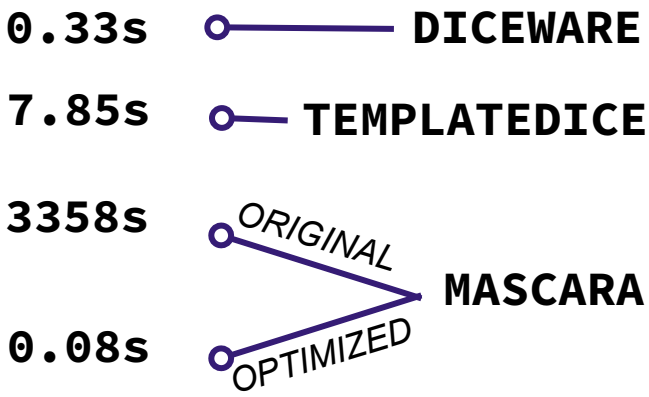
96% passphrases rejected by *PhraseMachine*, as not correct. Not much to show in results, thus removed. Word heuristics added.

Parameter Tuning

System parameters were manually set. Introduced new automated metric and performed grid search to remove bias and inaccuracies.

Time Complexity

Filtering and sampling word choices take linear query time. Improved it to logarithmic query time with linear preprocessing.



EVALUATION METRICS

SECURITY

Guessrank: No. of guesses adversary needs to crack passphrase. They use guessing algorithms.

Uses same cracking algorithm across all passphrase classes

Best of multiple cracking algorithms, close to real world process

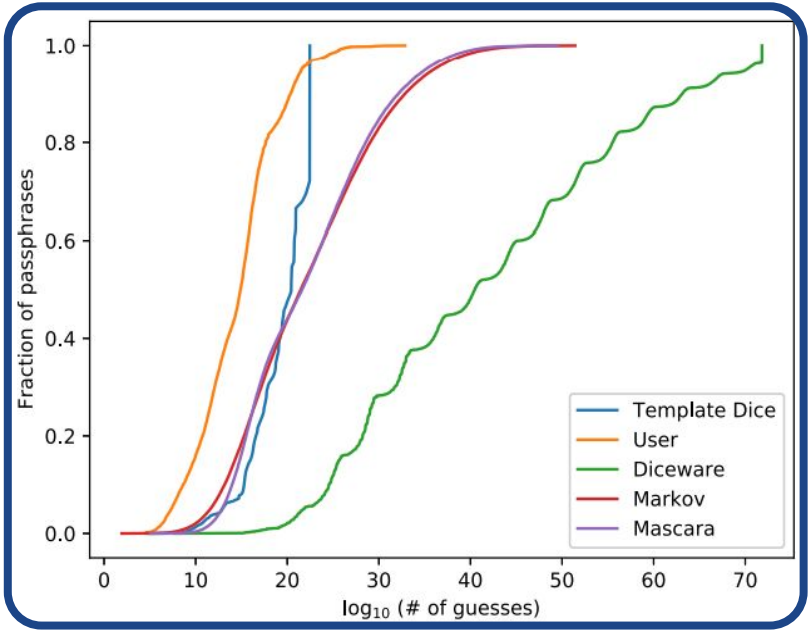
MEMORABILITY

CER: Character Error Rate, a proxy for memorability.

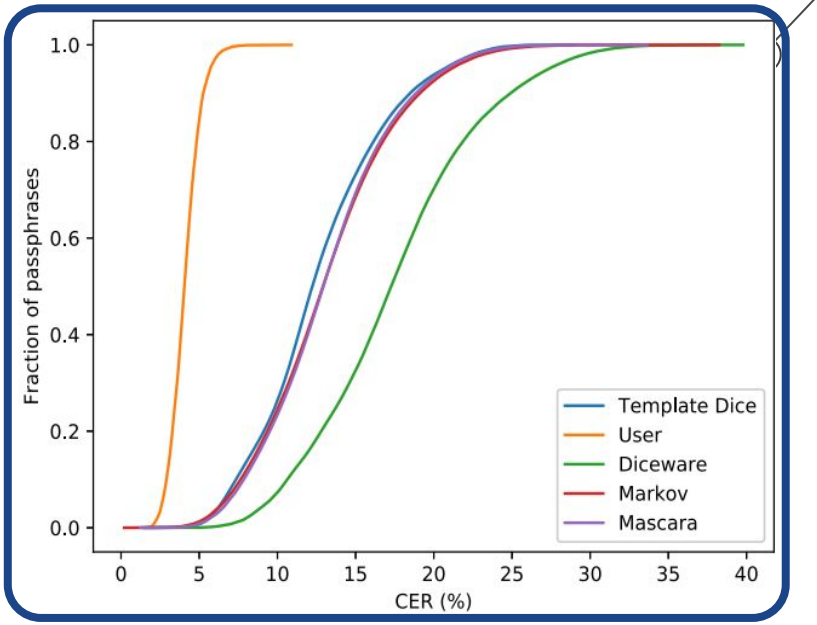
Uses theoretical claims to justify factors contributing to CER

Carry out experiments, using pearson correlation identify important factors for CER

RESULTS



Guessrank: Diceware highest (10^{40}), lowest User (10^{14}). Mascara better than TemplateDice after 40% pp



CER: Diceware highest (17%), lowest User (4%). Rest similar (around 12%).

Model	Recall	Mean CER	Median CER
Mascara	26.23%	34.78%	35.85%
TemplateDice	17.46%	35.44%	36.58%
Markov	21.95%	37.84%	41.27%
Diceware	24.00%	38.49%	42.57%

User Study

- Two part authentication survey.
- Highest Recall after 2 days: MASCARA.
- Diceware comparable due to lower return rate. High CER among returnees.

References

- Avirup Mukherjee. Systematic generation of secure and memorable passphrases, 2021.
- Ur, B., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., Komanduri, S., Kurilova, D., Mazurek, M.L., Melicher, W., & Shay, R. (2015). Measuring Real-World Accuracies and Biases in Modeling Password Guessability. USENIX Security Symposium.
- AG Reinhold. The diceware passphrase home page (1995). https://theworld.com/~reinhold/diceware.html.
- Make me a password. https://makemeapassword.ligos.net/. Accessed: 2022-01-31.
- Luis A Leiva and Germán Sanchis-Trilles. Representatively memorable: sampling the right phrase set to get the text entry experiment right. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 1709–1712, 2014.
- Simon S Woo. How do we create a fantabulous password? In Proceedings of The Web Conference 2020, pages 1491–1501, 2020.