PagPassGPT

Pattern Guided Password Guessing via Generative Pretrained Transformer

Reza Adinepour

Amirkabir University of Technology
(Tehran Polytechnic)

Computer Engineering Department

January 13, 2025

Agenda

1. Introduction
   - Problem & Solutions Overview
2. Main Contribution
3. Related Works
4. PagPass Methods
5. Evaluation
6. Results
   - Hit Rate
   - Repeat Rate

Problem & Solutions Overview

1. **Problem:** Deep learning-based password guessing models face challenges in:
   - Generating high-quality passwords.
   - Reducing the rate of duplicate passwords.
2. **Impact:** Reduced efficiency in password guessing models due to:
   - Lower hit rates.
   - High redundancy in generated passwords, limiting practical effectiveness.

Solutions

1. PagPassGPT:
    - Built on a Generative Pretrained Transformer (GPT).
    - Incorporates pattern structure information as background knowledge to improve guessing accuracy.
2. D&C-GEN (Divide-and-Conquer Generation):
    - Divides password guessing tasks into non-overlapping subtasks.
    - Subtasks inherit parent task knowledge for efficient prediction.
    - Effectively reduces duplicate passwords.
3. Results:
    - 12% higher hit rate compared to state-of-the-art models.
    - 25% fewer duplicate passwords.

Main Contribution

1. **PagPassGPT:**
   - Combines password patterns with deep learning.
   - Improves guessing accuracy.
2. **D&C-GEN:**
   - Uses divide-and-conquer for task splitting.
   - Reduces duplicate passwords.
3. **Performance:**
   - Validated on public datasets.
   - Outperforms state-of-the-art models in hit rate and duplicates.

Related works

1. **Password Guessing Types**
   - Trawling Attack:
     Problem: Misses rate patterns; requires accurate modeling.
   - Targeted Attack:
     Problem: Depends on personally identifiable information (PII); less effective with unpredictable users.
2. **Password Guessing Models**
   - Rule-based Models:
     Problem: Background knowledge dependency; limited rules.
   - Probability-based Models:
     Problem: Fixed vocabulary; poor segmentation accuracy.
3. **Deep Learning-based Models:**
   Problem: Accuracy loss; high computation.

PagPass Methods

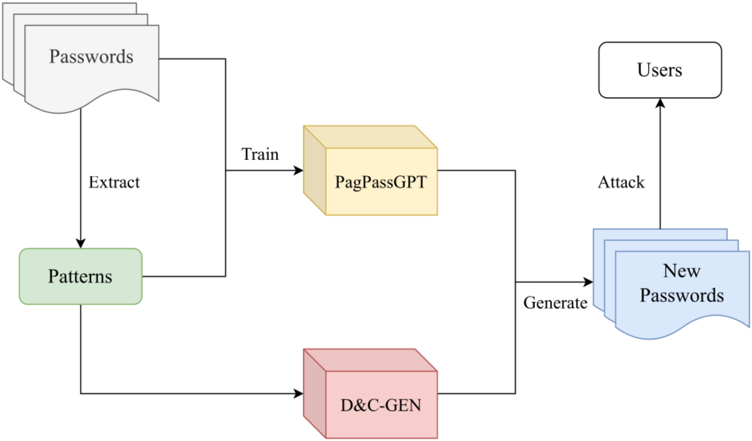


Figure: High-level idea of EDDI

Training Process

1. **Input:** Passwords from a training dataset.
2. **Training:**
   - Extract password patterns (e.g., "L4N3S1") using PCFG rules.
   - Combine patterns and passwords into a structured sequence: `<BOS> || Pattern || <SEP> || Password || <EOS>`
   - Tokenize sequences and embed using GPT-2 architecture.
   - Optimize with cross-entropy loss for improved prediction accuracy.

Training Process (Cont.)

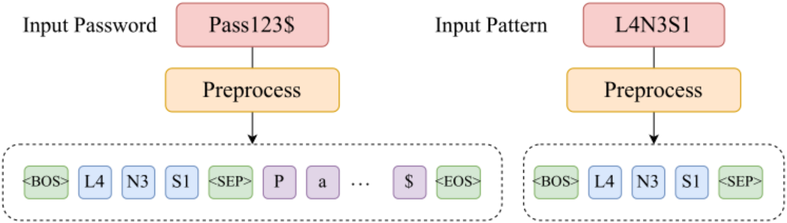


Figure: The preprocessing operation of tokenizer of PagPassGPT

Training Process (Cont.)

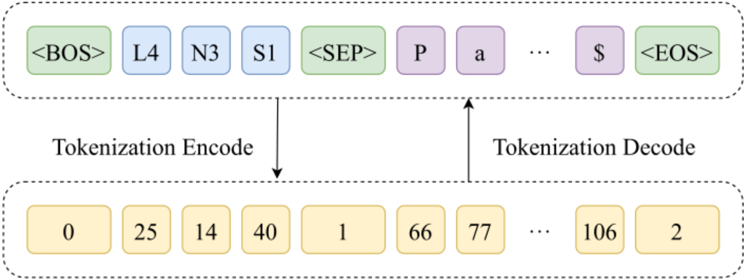


Figure: The tokenization process of the tokenizer of PagPassGPT

Training Process (Cont.)

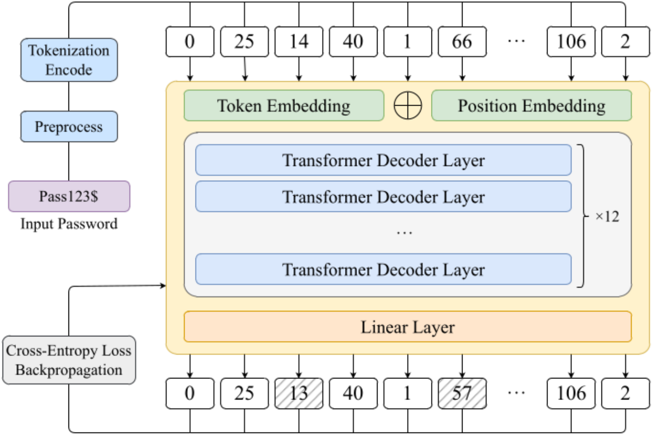
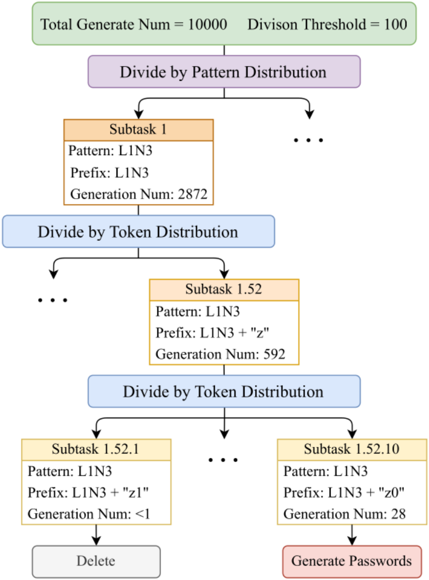


Figure: Training process architecture

D&C-GEN

1. **Objective:** Reduce duplicate passwords using divide-and-conquer.
2. **Workflow:**
   - Split tasks into non-overlapping subtasks by patterns and prefixes.
   - Apply a threshold T to stop division and execute generation.
   - Generate passwords efficiently under task constraints.
3. **Performance:**
   - Reduces duplicate rate to 9.28% for 10^9 guesses.
   - Supports parallel execution and optimized GPU utility.

D&C-GEN (Cont.)


Total Generate Num = 10000 Divison Threshold = 100
Divide by Pattern Distribution
Subtask 1
Pattern: L1N3
Prefix: L1N3
Generation Num: 2872
. . .
Divide by Token Distribution
. . .
Subtask 1.52
Pattern: L1N3
Prefix: L1N3 + "z"
Generation Num: 592
Divide by Token Distribution
Subtask 1.52.1
Pattern: L1N3
Prefix: L1N3 + "z1"
Generation Num: <1
. . .
Subtask 1.52.10
Pattern: L1N3
Prefix: L1N3 + "z0"
Generation Num: 28
Delete
Generate Passwords

Evaluation

1. **Datasets**
   - Ethical Considerations:
     - Public data, minimal usage, and strictly for research purposes.
   - Applied Datasets:
     - RockYou, LinkedIn, phpBB, MySpace, Yahoo!
     - Total entries: 75,349,874.
   - Data Cleaning:
     - Password length: 4–12 characters.
     - Removed duplicates and non-ASCII characters.
   - Data Utilization:
     - RockYou & LinkedIn: Split into training (70%), validation (10%), and testing (20%).
     - Cross-site evaluation: Used all remaining datasets.

Evaluation (Cont.)

1. **Models**
   - PagPassGPT:
     - Trained with batch size 512 for 30 epochs using AdamW optimizer.
     - Max tokens: 32, Embedding size: 256.
     - Hidden layers: 12, Attention heads: 8.
     - Training duration: 25+ hours on 4 RTX 3080 GPUs.
2. **Drawling Attack Test**
   - Setup:
     - Compared PagPassGPT and PagPassGPT-D&C (with threshold $T = 4000$) against models like PassGAN, VAEPass, PassFlow, and PassGPT.

Evaluation (Cont.)

1. **Metrics**
   - Hit Rate:
     - Ratio of correctly guessed passwords to total test set passwords.
     - PagPassGPT-D&C achieved a 53.63% hit rate for 10^9 guesses, 12% higher than PassGPT.
   - Repeat Rate:
     - Reflects duplicate passwords among generated ones.
     - PagPassGPT-D&C achieved a 9.28% repeat rate, significantly lower than PassGPT's 34.5%.

Hit Rate

Table: Hit rates of different models in trawling attack test.

Guess Num	10^6	10^7	10^8	10^9
PassGAN	0.80%	3.11%	8.24%	16.32%
VAEPass	0.49%	2.24%	6.24%	12.23%
PassFlow	0.26%	1.62%	7.03%	14.10%
PassGPT	0.73%	5.60%	21.43%	41.93%
PagPassGPT	1.00%	7.68%	27.23%	48.75%
PagPassGPT-D&C	**1.05%**	**8.48%**	**31.38%**	**53.63%**

Repeat Rate

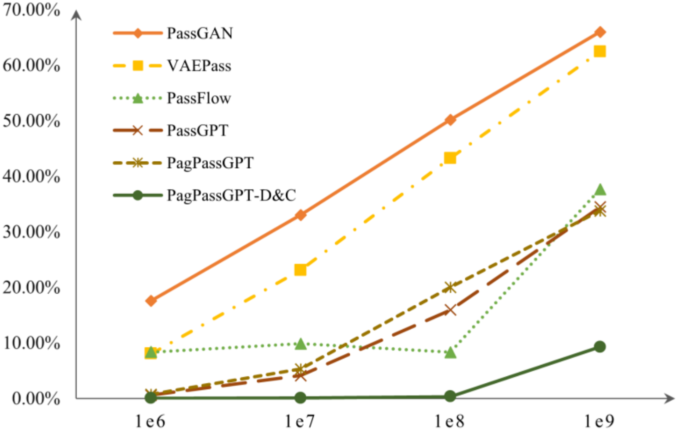


Figure: Repeat rates of passwords generated by different models

References

Xingyu Su, Xiaojie Zhu, Yang Li, Yong Li, Chi Chen, Paulo Esteves-Veríssimo (2024)
PagPassGPT: Pattern Guided Password Guessing via Generative Pretrained Transformer
arXiv:2404.04886v2 [cs.CR], School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China; Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China; King Abdullah University of Science and Technology, Thuwal, Kingdom of Saudi Arabia.
Emails: {suxingyu, liyang8119, liyong, chenchi}@iie.ac.cn, {xiaojie.zhu, paulo.verissimo}@kaust.edu.sa.

The End

Questions? Comments?

adinepour@aut.ac.ir