Keys Your Account Goodbye: Semi-Targeted Password Cracking via Keywords

Beitong Tian[†], **Jaron Mink**[†], **Jason Liu**[†], **Gang Wang**
Department of Computer Science, University of Illinois at Urbana-Champaign
[†]co-authors

Introduction

Prior Work
- Untargeted Methods
  - No knowledge of target
  - e.g.: JTR, CFG, Markov Chains, Neural Net
- Targeted Methods:
  - Detailed knowledge of individuals
  - e.g.: omen+, Personal-PCFG, TarGuess

Key Insight
- Passwords may be related to the interest of the website
- Personal info may not be required for increased guessing efficiency

Threat Model
Two models:

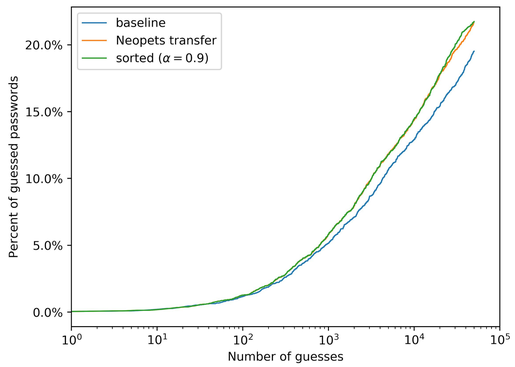
1. Attacker with access to password leak of site belonging to same interest group (strong)
2. Attacker without access to any private data, only websites and forums related to interest group (weak)

Method

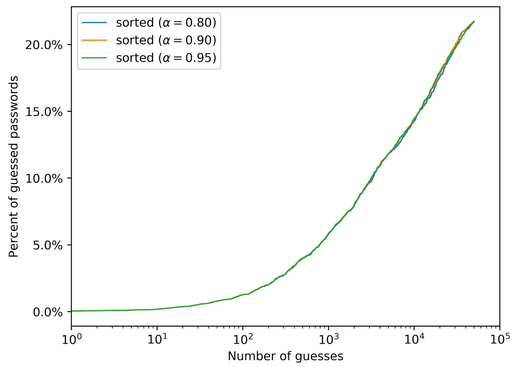
- Using open-source model from *Melicher et al.*, 2016 on Github
- **Baseline**: pre-trained model
  - Ordered via descending probability
- **Transfer learning** on different password sets
  - Retrain while freezing feature layers
  - Ordered via descending probability
- **Keyword Sorted**
  - Keywords selected manually
  - Ordered via descending keyword similarity-probability weighting:

    order_weight = **α**(prob) + (1-**α**)(keyword_sim)
- Similarity algorithm based on minimum password-keyword Levenshtein distance.

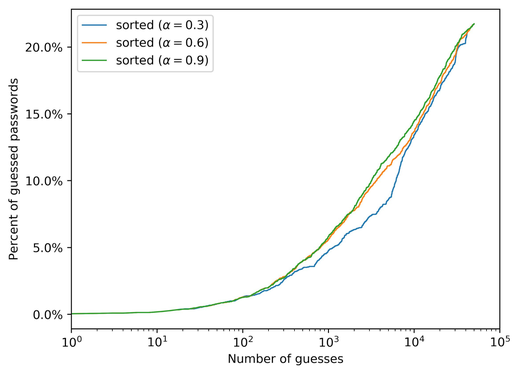
Results



Target passwords are from the forum Neofriends, while the transfer model was trained using Neopets.

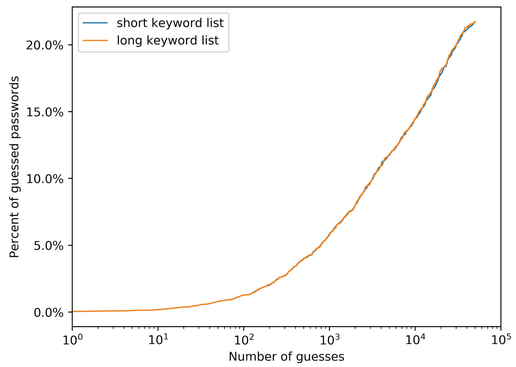


Comparison of α near 0.9, using the intuition that around 10% of passwords contain keywords.

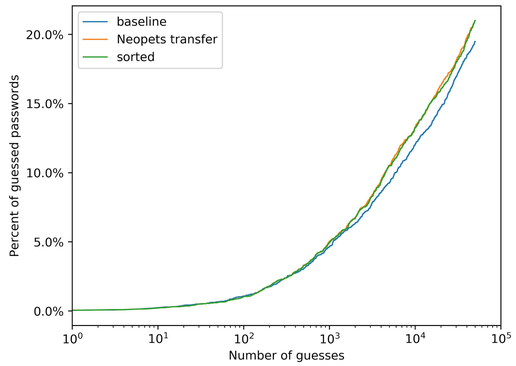


Comparison of α in a wider range. Values too small (i.e. favoring keywords too heavily) reduce performance as common general passwords, such as "123456789" or "password", are missed.

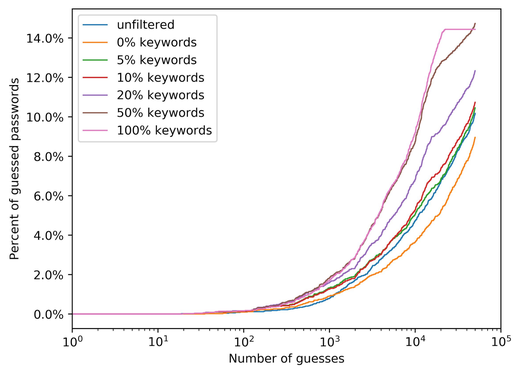
Results Cont.



Comparison of a "short" keyword list (only animal names, 145 words) with a "long" keyword list (includes Neopets keywords and more animals, 1308 words).



"Cross-set" test: the target passwords come from "CrackingForum", while the transfer learning was done on Neopets.



Idealized results when considering target lists with specific keyword densities. (Each keyword density list is the Neopets dataset with entries filtered until X% are considered strongly related by Levenshtein distance.)

Limitations

- Failed Methods: transfer learning on some data sets
  - Attacker model 2: training on keywords results in gibberish passwords (e.g. "<=>?#_:;")
    - potentially bug and/or bad training
- Keywords are manually created via human intuition of the subject
  - Not comprehensive by any means
- Not all password sets seem to be related to a specific interest
  - e.g.: large social media sites

Future Work

- Create a quantifiable metric to describe similarity between website and interest group/keywords
  - "Why do we train on X and target Y?"
- Successfully transfer learn and guess on keywords only (attacker model 2)
- Create a principled way to discover keywords
  - knowledge graph queries
  - web scraping related forums/website + NLP keyword algorithms
- Test if smaller, more niche websites have higher frequency of keywords and thus are more vulnerable
- Determine if there's a difference between keyword reordering vs increased training (higher epochs, non-transference)
- Create a password guessability trained for specific websites

Acknowledgments
Thanks to Gang Wang for guidance and providing the password data, and Melicher et al. for the open-source password guessing model upon which this project is based.

ILLINOIS