Personalized Password Guessing

Phuong Cao, Hongyang Li, Adam Slagell, Klara Nahrstedt, Zbigniew Kalbarczyk

Coordinated Science Laboratory & National Center for Supercomputing Applications • University of Illinois at Urbana-Champaign

## Background

### Text-based passwords
Users often choose simple, dictionary-based passwords.

### Attacks targeting passwords
The number of password leaks is increasing recently, e.g., LinkedIn (5M), Adobe (150M).

### Existing work on passwords
Existing works measure construction rules and strength of passwords without taking into account of user profiles and the service that requires passwords.

## System Workflow

### Generating P personalized words
A word $w_0$ is selected from a topic $t_p$. The topic is based on a list of user profile topics $t_u$ and a list of service topics $t_s$. A topic distribution is parameterized by $\theta$ and a word-topic distribution is parameterized by $\phi$.

### Generating a personalized password
From $P$ personalized words based on grammatical and mangling rules.

## Experiments

### Personalized password guessing
- **Design**: using questionnaire forms to collect user profiles and ask users to generate passwords for several types of services.
- **Goal**: identify the relationships between the user/service profile and the generated passwords.

### Personalized password generation
- **Design**: using a sign-up or change password form to suggest personalized passwords to a user.
- **Goal**: suggest personalized passwords and measure strength of a password provided by a user.

## Research Question

### Question
Is personalized password cracking a better approach compared to dictionary based or random guess approaches?

### Goal
Evaluate the viability of cracking a user password faster using user/service profile.

### Hypothesis
A user generates a password based on a list of words, each is drawn from a topic related to the user.

### Approach
Using probabilistic graphical model to capture relationships between the user password and the user/service profile.

Running survey on real users to validate our hypothesis.

## Applications

1. Suggest personalized, secure, and easy to memorize passwords to users.
2. Measure strength of a password using personalized metrics.

## Conclusion

A probability based framework to automate generation of personalized passwords based on user and service profiles.

Two experiments are designed to:
- Evaluate the viability of cracking a user password faster using user/service profile.
- Suggest personalized, secure, and easy to memorize passwords to users.

## Acknowledgements

This work was supported in part by NSF grant CNS 10-18503 CISE and 1314891, by the Army Research Office under Award No. W911NF-13-1-0086, the National Security Agency (NSA) under Award No. H98230-14-C-0141, Air Force Research Laboratory and the Air Force Office of Scientific Research, under agreement No. FA8650-11-2-0084.

## References