Allowing Typos in Passwords… good or bad

Examining password security under a typo tolerant system

Ben Smith†  
 CS&E  
 University of Minnesota - Twin Cities  
 Minneapolis, MN  
 smit9524@umn.edu

Matt Strapp  
 CS&E  
 University of Minnesota - Twin Cities  
 Minneapolis, MN  
 strap012@umn.edu

Ayo Osonowo  
 CS&E  
 University of Minnesota - Twin Cities  
 Minneapolis, MN  
 osono003@umn.edu

Noah Zimmerman  
 CS&E  
 University of Minnesota - Twin Cities  
 Minneapolis, MN  
 zimm0508@umn.edu

Jack Poehlmann  
 CS&E  
 University of Minnesota - Twin Cities  
 Minneapolis, MN   
 poehl083@umn.edu

ABSTRACT

We examine the security of the TypTop personalized typo tolerant password checking system by having it fight with a relatively strong password guessing system OMEN. TypTop has a caching algorithm it uses to learn user’s most common password typos and allow them. We performed an offline guessing attack by using the TypTop caching algorithm to setup a cache state and running the OMEN system against this cache state. We found this to be a secure system, despite initial concerns about security.

CCS CONCEPTS

• Password security • Cryptographic security   • Enumerative Markov model

1 INTRODUCTION

A survey of the modern internet will find passwords used extensively compared to other forms of authentication, such as biometrics or two-factor. Passwords remain prevalent due to their ease of implementation from both a user and a technical side; the average number of passwords an individual has in 2021 is \_\_\_\_\_ (**source**). However, their ease-of-use leads to security flaws as well: often users will choose easy-to-remember passwords because the task of remembering \_\_\_ passwords is too much. Strides in modern cryptography and security have also impacted “attacker” security research, and the general majority of user passwords are easily cracked (**source**) via brute-force, dictionary, and other more complex attacks. It is for this reason that users are encouraged to choose robust passwords that conform to a set of recommendations (for example, longer than 16 characters, use special symbols, use a combination of upper and lowercase characters, alphanumeric passwords). Longer, more complex passwords see a higher rate of typos [2]. A study by Chatterjee et. al in 2016 showed that 9.3% of login attempts for Dropbox users were denied based on small, easy to correct typos. Some typo tolerant password checking systems are already implemented, such as the system by Facebook that allows common typos like accidentally leaving caps lock on, or mis-capitalizing the first character. However, the most prevalent typos only account for 20% of password typos made by users, leaving the majority unaccounted for. Enter TypTop (pronounced: “tip top”), a typo tolerant password checking system that learns users’ most common password typos, and will overlook them. The cryptographic security of this system is well-documented, and we seek not to examine this aspect of security of the TypTop system, but examine instead the usability and customizability of the system to provide an optimally secure yet tolerant system. We will explore users’ perceptions on such a system, as well as implications of altering cache size, caching schemes, and methods for ‘warming up the cache.’ The easiest way to do this is through an offline “attack” in which we can model the state of TypTop at a given point, and measure the ease in which a password guessing tool is able to either guess the password or one of its allowable typos. We can successfully model the cache state by following the caching policies laid out in Chatterjee et. al’s paper (**source**). The password guessing tool we use is called OMEN (Ordered Markov ENumerator) (**source**), and is a probabilistic algorithm based on the Markov model used to generate passwords in decreasing order of likelihood of being used.

2 OVERVIEW OF THE TYPTOP SYSTEM

The TypTop system utilizes a cache of most common typos to learn what mistakes a user makes most. Many attributes of the cache can be set at runtime, and include caching policy, cache size, and schemes for “warming up” the cache. A separate “wait list” of typos is maintained to determine the frequency of typos and what should eventually be admitted to the cache. Both the cache and the wait list are cryptographically secure, and have been extensively proved in Chatterjee et al.’s work [1].

ACKNOWLEDGMENTS

We would like to thank the University of Minnesota’s Computer Science and Engineering department for supporting this research, as well as our CSCI5271 instructor Stephen McCamant. We would also like to thank Drs. Chatterjee and Duermuth for supplying the source code for TypTop and OMEN, respectively.

REFERENCES

[1] Rahul Chatterjee, Joanne Woodage, Yuval Pnueli, Anusha Chowdhury, and Thomas Ristenpart. 2017. The TypTop System: Personalized Typo-Tolerant Password Checking. In CCS’17. CCS’17, 329-346

[2] Rahul Chatterjee, Anish Athalye, Devdatta Akhawe, Ari Juels, and Thomas Ristenpart. 2016. pASSWORD tYPOS and How to Correct Them Securely. *IEEE Symposium on Security and Privacy* (may 2016).

[3] Sarah Pearman, Jeremy Thomas, Pardis Emani Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. 2017. Let’s Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In CCS’17. CCS’17, 295-310.

[4] Briland Hitaj, Paolo Gasti, Giuseppe Ateniese, and Fernando Perez-Cruz. 2018. PassGAN: A Deep Learning Approach for Password Guessing. *NeurIPS 2018 Workshop on Security in Machine Learning*. SecML’18.

[5] Markus Duermuth, Fabian Angelstorf, Claude Castelluccia, Daniele Perito, Abdelberi Chaabane. OMEN: Faster Password Guessing Using an Ordered Markov Enumerator. International Symposium on Engineering Secure Software and Systems, Mar 2015, Milan, Italy. hal-01112124f

Conference Name:ACM Woodstock conference

Conference Short Name:WOODSTOCK’18

Conference Location:El Paso, Texas USA

ISBN:978-1-4503-0000-0/18/06

Year:2018

Date:June

Copyright Year:2018

Copyright Statement:rightsretained

DOI:10.1145/1234567890

RRH: F. Surname et al.

Price:$15.00