pASSWORD tYPOS and How to Correct Them Securely

Project Silver

Rahul Chatterjee, Anish Athayle, Devdatta Akhawe, Ari Juels, Thomas Ristenpart

rahul@cs.cornell.edu

Introduction

Typos are annoying.

Websites reject a login attempt even if a legitimate user makes small typographical mistakes when typing password. This hampers user experience and discourages users from choosing long passwords.

We analyze the usability benefits and security loss of tolerating small typographical errors in submitted passwords.

Usability	Security
Fraction of login attempts results in successful login.	Success probability of an attacker in guessing a randomly sampled password within q tries.

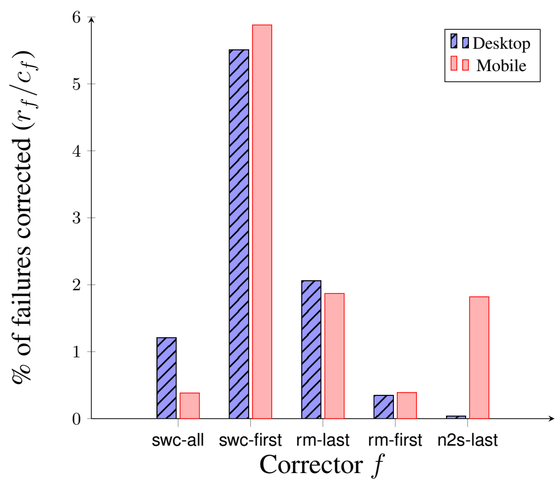
Typo Rates

Collected typo data using studies conducted at:

- Amazon Mechanical Turk, and
- Dropbox login infrastructure

Dropbox results:

- 9% of all the logins fail due to 3 typos, such as accidental pressing caps-lock key.
- fixing these simple typos can increase total login by 3% in Dropbox.
- delay in login can be saved by 100 seconds for 20% of the users.



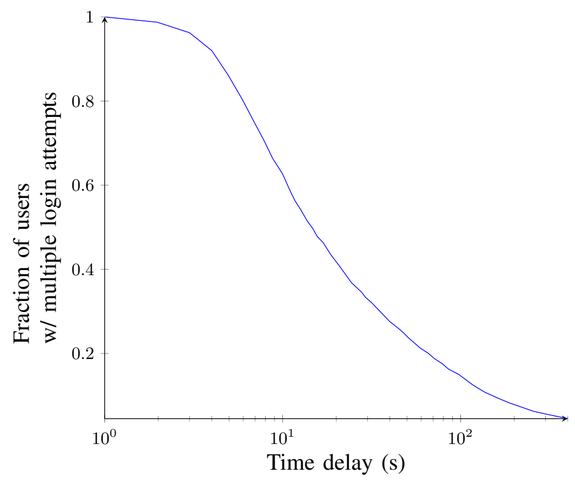


Figure: (**Left**) Fraction of failed logins due to some easily correctable typos. (**Right**) Fraction of logins delayed due to those easily correctable typos.

Typo Correction

Correctors: A set of simple transformation functions that corrects *easily correctable typos*.
e.g., `swc-all`, switches the case of all the letters in a password.

Correcting typos on the fly:
Allow login if either the entered password or any of the corrected versions of it matches the stored password.
Compatible with existing password stores, and:

1. Offline attack remains unchanged.
2. Online attack can be throttled by the website if the website sees a lot of failed login attempts.

- Our **free corrections theorem** proves that one can correct typos without any security loss, in theory
- We provide practical typo tolerant password checkers based on the theory

Security

Security Degradation

$$\Delta_q = \lambda_q^{\texttt{fuzzy}} - \lambda_q$$

	Attacker distribution	Challenge distribution		
		RockYou	phpBB	Myspace
Only entered password	RockYou	11.23	3.21	9.34
	phpBB	8.10	12.71	1.81
	Myspace	3.57	3.32	9.54
Try all typo correctors	RockYou	+0.51	+0.28	+0.25
	phpBB	+0.25	+0.38	+0.11
	Myspace	**-0.15**	**-0.02**	+0.49
Fix typos except to blacklisted PWs	RockYou	+0.32	+0.11	+0.20
	phpBB	+0.06	+0.19	+0.05
	Myspace	**-0.26**	**-0.20**	+0.46
Fix typos except for heavy balls	RockYou	0.00	0.00	0.00
	phpBB	**-0.11**	+0.15	**-0.04**
	Myspace	**-0.27**	**-0.14**	+0.35

Conclusion

Typo correction in passwords is possible with negligible degradation in security.