Poster: The last step of password strength evaluation

Yan Shao
University of International Relations
y_shao@uir.edu.cn

Xin Xin
University of International Relations
grace_xin77@163.com

Hong Di*
University of International Relations
di_hong@163.com

***Abstract*—Passwords are typically the first line of protection in a security system, yet they are also the most vulnerable. The key to ensuring security is to use strong passwords. The security systems encourage users to create strong passwords through password strength estimation. There is no doubt that the existing password strength estimate methods are already very accurate for the identification of the weak passwords. However, among the passwords that meet their strong password condition, there are still some misjudged passwords. In this poster, we propose Character Distance Strong Password Checker (CDSPC). Specifically, Consecutive Lead Character Distance (CLCD) and Average Adjacent Character Distance (AACD) are used in CDSPC. CLCD is the sum of distance between all characters and the first character in the password. And AACD is the average value of every two adjacent characters distance in the password. The types of characters contained in the password and the lengths of password are recognized by CLCD, while the permutations of characters in the password are recognized by AACD. In the experiment, CDSPC was able to distinguish a misjudged strong password that had been evaluated as strong password using the password strength evaluation methods LPSE and ZXCVBN.**

I. INTRODUCTION

Passwords are essential for safeguarding information property. Text password occupies an irreplaceable position in the Internet because of its convenience and low cost [1]. As the Internet grows in popularity, so does the number of weak passwords. There have been three primary ways to limit the spread of weak passwords in recent years. The first is for the system to create user passwords that are not only lengthy enough but also random enough [2], [3]. In general, users do not need to memorize such complicated passwords but rely on third-party password storage services. Users would face new authentication and trust issues as a result of a third-party involvement. The second type of password rules are set by the web administrator [4]. The length and character type of passwords are typically governed by the regulations, in order to register properly, the users must adhere to them. This coercive approach does improve password strength, but previous research indicated that users can only fulfill the regulations' minimal requirements, thus it does not play a positive role. The third is to use a password strength evaluation method on the registration interface [5] that can provide real-time feedback on password strength in the form of text [strong, medium, weak] or a colored bar. Users can only register if their passwords satisfy the specified strength requirement. Previous researches [6] have shown that when users are aware of the strength of passwords, they will actively use various characters to construct stronger passwords.

The existing password strength evaluation methods will evaluate the passwords as unreasonable strength [7]. Obviously, judging weak passwords as strong is more dangerous. The Internet suffers greatly as a result of the incorrect classification of weak password intensity levels. For the same input password, different password strength evaluation methods will produce different output strengths, leaving users perplexed while creating passwords for several websites [8]. The existing password strength evaluation methods, according to Wang $et\ at.$ [9], are ineffective in detecting weak passwords. Research by Ur $et\ at.$ [10] showed that password strength may be significantly enhanced only if a password strength meter is provided with accurate strength.

In order to increase the accuracy of the password strength as much as possible, there are two password strength evaluation methods: one is ZXCVBN [11] which from industry, the other is LPSE [12] which from academia. Although the above-mentioned password strength evaluation methods have high accuracy, there are still some misjudgment in the strong passwords. We present Character Distance Strong Password Checker (CDSPC) to identify this part of misjudged passwords. Specifically, CDSPC calculates the character distance of the password to determine whether its strength is evaluated correctly. Two character distances are utilized in particular: Consecutive Lead Character Distance (CLCD) and Average Adjacent Character Distance(AACD). In the experiment of calculating the character distance of strong passwords, two password strength evaluation methods from different datasets are selected, the experimental results show that the proposed method is effective in identifying misjudged passwords.

II. METHODOLOGY

A. Character Distance

In order to distinguish the type of character effectively, we need to redesign the value of the character, which is called pivot value. As shown in Table.I, since the continuous length of lowercase and uppercase letters is 26, the minimum difference between $[\zeta_1, \zeta_2, \cdots, \zeta_{26}]$ and $[\xi_1, \xi_2, \cdots, \xi_{26}]$ should be at least 26 in order to reflect the change of character types. Similarly, the minimum difference between $[\varsigma_1, \varsigma_2, \cdots, \varsigma_{10}]$ and $[\zeta_1, \zeta_2, \cdots, \zeta_{26}]$ should also be at least 26. Obviously, the minimum difference between $[\xi_1, \xi_2, \cdots, \xi_{26}]$ and η should be at least the number of symbols.

* Hong Di is corresponding author.

TABLE I
PIVOT VALUE OF CHARACTERS

Characters	Pivot value
$[0, 1, \cdots, 9]$	$[\varsigma_1, \varsigma_2, \cdots, \varsigma_{10}]$
$[a, b, \cdots, z]$	$[\zeta_1, \zeta_2, \cdots, \zeta_{26}]$
$[A, B, \cdots, Z]$	$[\xi_1, \xi_2, \cdots, \xi_{26}]$
symbols	η

With the pivot value of characters, for any two characters α and β, the character distance is renewed to:

$$distance(\alpha, \beta) = |PV(\alpha) - PV(\beta)|, \tag{1}$$

in which $PV(\chi)$ represents the pivot value of character χ.

B. Two Indicators Based on Character Distance

The factors that affect the strength of a password are not only the characters which compose the password, but also the permutation of the characters. Specifically, for a password composed of multiple characters, it is necessary to consider the length of the password, the type of internal characters, the proportion of the same type characters, and the permutation of characters.

In order to take these factors into account, two indicators are proposed in this poster. One is CLCD, the other is AACD, the definition of them are as follows:

$$CLCD = \sum_{i=0}^{i<n} |P[i] - P[0]|, \tag{2}$$

in which P represents the password and $P[x]$ represents the character with index x in the password.

In CLCD, the password length with the same character type can be determined by the sum operation. For example, $Xbox360PS2021NS$ and $Xbox360PS2021NSOLED$ are composed of the same character type, the CLCD value of the former is significantly smaller than that of the latter. Another advantage of CLCD is that it is sensitive to the proportion of the same type characters in passwords. For example, if there are passwords $sourGRAPS$ and $sourgraps$, due to the large gaps between the pivot values of different character types, CLCD can calculate the proportion of lowercase letters and uppercase letters in the former, while knowing there are only lowercase letters in the latter.

$$AACD = \sum_{i=1}^{i<n} |P[i] - P[i-1]|. \tag{3}$$

The AACD uses averages in its calculation, so it is not possible to measure the effect of password length on password strength. However, AACD does a good job of recognizing permutation in character types of passwords. For example, there are both passwords $AaAaAaAa$ and $AAAAaaaa$ with the same value of CLCD. Even though they both have the same characters, the former character type changes more often than the latter. Therefore, the AACD value of the former is higher than that of the latter.

C. Checking Strong Password

CLCD and AACD evaluate password strength from different perspectives. Therefore, to evaluate the strength of a given password accurately, it is necessary to calculate not only the two character distances, but also the threshold of two proposed indicators indicators. It is worth mentioning that the threshold is different for different datasets. We analyze the distribution of characters in different datasets with different password strength evaluation methods to determine the threshold. Finally, whether the strength level of the strong password has changed is determined by judging the threshold of two character distances.

ACKNOWLEDGMENTS

This work was specially supported by National Natural Science Foundation of China (62102113), Fundamental Research Funds for the Central Universities (3262021T25), and Undergraduate Academic Support Program of the University of International Relations (3262021SYJ006, 3262021SYJ001).

REFERENCES

[1] S. Murmu, H. Kasyap, and S. Tripathy, "Passmon: A technique for password generation and strength estimation," *Journal of Network and Systems Management*, vol. 30, no. 1, pp. 1–23, 2022.

[2] M. N. Al-Ameen, K. Fatema, M. Wright, and S. Scielzo, "The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 185–196.

[3] J. H. Huh, S. Oh, H. Kim, K. Beznosov, A. Mohan, and S. R. Rajagopalan, "Surpass: System-initiated user-replaceable passwords," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 170–181.

[4] R. Shay, S. Komanduri, A. L. Durity, P. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Designing password policies for strength and usability," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 4, pp. 1–34, 2016.

[5] R. Shay, L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, and B. Ur, "A spoonful of sugar? the impact of guidance and feedback on password-creation behavior," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 2903–2912.

[6] M. Golla and M. Dürmuth, "On the accuracy of password strength meters," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1567–1582.

[7] L. David and A. Wool, "An explainable online password strength estimator," in *European Symposium on Research in Computer Security*. Springer, 2021, pp. 285–304.

[8] Q. Dong, C. Jia, F. Duan, and D. Wang, "Rls-psm: A robust and accurate password strength meter based on reuse, leet and separation," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4988–5002, 2021.

[9] D. Wang, D. He, H. Cheng, and P. Wang, "fuzzypsm: A new password strength meter using fuzzy probabilistic context-free grammars," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2016, pp. 595–606.

[10] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "" i added'!'at the end to make it secure": Observing password creation in the lab," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 123–140.

[11] D. L. Wheeler, "zxcvbn: Low-budget password strength estimation," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016, pp. 157–173.

[12] Y. Guo and Z. Zhang, "Lpse: lightweight password-strength estimation for password meters," *computers & security*, vol. 73, pp. 507–518, 2018.

Poster: The last step of password strength evaluation

Yan Shao
University of International Relations
y_shao@uir.edu.cn

Xin Xin
University of International Relations
grace_xin77@163.com

Hong Di
University of International Relations
di_hong@163.com

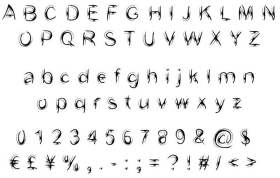
"The motivation of this poster is to identify the part of the misjudged passwords that hide in the strong passwords. In this poster, we propose Character Distance Strong Password Checker (CDSPC). Specifically, Consecutive Lead Character Distance (CLCD) and Average Adjacent Character Distance (AACD) are introduced in CDSPC."

Research Problem

- Among the passwords which are identified as strong passwords, some of them maybe not satisfy the strong evaluation condition.
- Medium strength passwords or weak strength passwords that are misjudged as strong passwords will bring inestimable harm to the cyberspace or computer systems.

Our Approach

1.Evaluation Indicators



PIVOT VALUE OF CHARACTERS

Characters	Pivot value
$[0, 1, \cdots, 9]$	$[\varsigma_1, \varsigma_2, \cdots, \varsigma_{10}]$
$[a, b, \cdots, z]$	$[\zeta_1, \zeta_2, \cdots, \zeta_{26}]$
$[A, B, \cdots, Z]$	$[\xi_1, \xi_2, \cdots, \xi_{26}]$
symbols	η

$$CLCD = \sum_{i=0}^{i<n} |P[i] - P[0]|, \qquad AACD = \sum_{i=1}^{i<n} |P[i] - P[i-1]|.$$

AACD and CLCD reflect the comprehensive quality of passwords.

2.Determining Pivot Value

The number of passwords contained in each dataset

	Dataset	Quantity
Native speakers of English	hotmail	8,931
	myspace	37,144
	rockyou	14,344,391
	yahoo	5,000,136
Native speakers of Chinese	csdn	6,426,875
	duduniu	16,283,140
	renren	4,768,600
	tianmao	3,036,273
	7k7k	19,138,452
	178	9,072,966

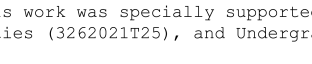
Over the past few years, real passwords have been leaked for various reasons. The leaked password datasets provide a great aid to password cracking technology. We choose the password datasets leaked in recent years to determine pivot value of password strength evaluation method proposed in this poster.

Final pivot value of characters

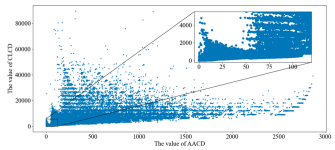
	Pivot value	
	hotmail, myspace, rockyou, renren	yahoo, csdn, duduniu, tianmao, 7k7k, 178
$[0, 1, ..., 9]$	[120, 121, ..., 129]	[60, 61, ..., 69]
$[a]$	[3]	[100]
$[e, o, i, r, l, n, s]$	[7, 8, ..., 13]	[200, 201, ..., 206]
$[t, m, c, u, d, b, p, h, g, y]$	[18, 19, ..., 27]	[300, 301, ..., 309]
$[v, k, f, j, z, x, w, q]$	[53, 54, ..., 60]	[400, 401, ..., 407]
$[A, B, ..., Z]$	[900, 901, ..., 925]	[1500, 1501, ..., 1525]
Symbols	3000	3000

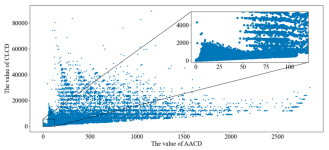
3.Checking Strong Password

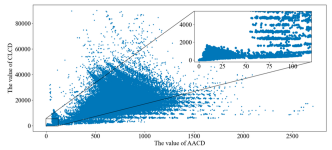
CLCD and AACD values evaluate password strength from different aspects. Therefore, to evaluate the strength of a given password accurately, it is necessary to calculate not only the distance between two characters, but also the threshold of two proposed indicators. Combining with the existing password strength evaluation method, the CLCD value and AACD value of a password are calculated through the pivot value to determine whether it is evaluated accurately.

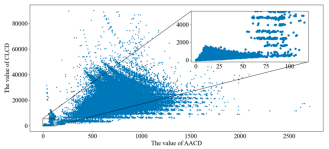


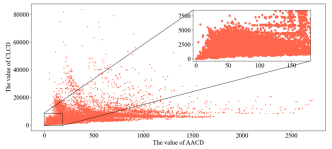
Real Dataset Experimental Results

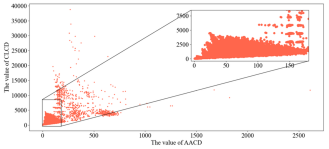

Strong passwords evaluated by LPSE from rockyou

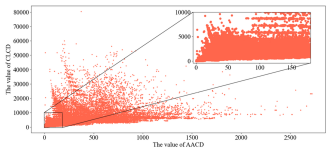

Strong passwords evaluated by ZXCVBN from rockyou

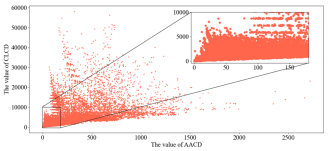

Strong passwords evaluated by LPSE from renren


Strong passwords evaluated by ZXCVBN from renren


Strong passwords evaluated by LPSE from duduniu


Strong passwords evaluated by ZXCVBN from duduniu


Strong passwords evaluated by LPSE from yahoo


Strong passwords evaluated by ZXCVBN from yahoo

We choose strong passwords from the password strength evaluation methods both in theory and industry, that are LPSE and ZXCVBN. Then the CLCD and AACD values of these strong passwords are evaluated respectively, and the change of density is observed to find the passwords which do not match the strength.

Top 2 patterns and probalities of misjudged passwords from LPSE and ZXCVBN

	LPSE		ZXCVBN	
	Pattern	Prob.	Pattern	Prob.
hotmail	M	0.527	M	0.257
	MD4	0.055	D9	0.185
myspace	M	0.452	MD2	0.201
	MD4	0.059	MD1	0.144
rockyou	M	0.337	D10	0.272
	MD4	0.080	M	0.181
renren	M	0.282	D11	0.419
	MD6	0.076	D9	0.293
csdn	M	0.246	D11	0.273
	MD6	0.103	D9	0.173
tianmao	M	0.077	D11	0.445
	D11M	0.074	D9	0.163
7k7k	M	0.227	D9	0.345
	MD6	0.078	D11	0.215
178	MD6	0.176	D11	0.328
	M	0.155	D9	0.208
duduniu	M	0.111	A2D7	0.110
	MD7	0.078	A1D8	0.092
yahoo	A1D11	0.066	A1D10	0.212
	A4D8	0.047	A1D8	0.170

In order to demonstrate CDSPC's ability of identifying misjudged passwords, we use the password cracking tool Next-gen PCFG to analyze the misjudged passwords patterns. Specifically, we train password patterns from misjudged passwords in LPSE and ZXCVBN and then observe the top 2 patterns and probabilities as shown in left table.

M denotes multi-words, D denotes digits, and A denotes alphabets in Next-gen PCFG. It is easy to see that there are a large number of M patterns in the misjudged passwords of LPSE, while ZXCVBN has a large number of D patterns.

Conclusion

- Our proposed method takes O(n) time to calculate the character distance.
- CDSPC can be deployed on both client and server because of its lightweight feature.
- Experiments results show that our CDSPC can identify misjudged passwords effectively.
- Combining with the state-of-the-art password strength evaluation methods, CDSPC can achieve an outstanding password strength evaluation results.

This work was specially supported by National Natural Science Foundation of China (62102113), Fundamental Research Funds for the Central Universities (3262021T25), and Undergraduate Academic Support Program of the University of International Relations (3262021SYJ006, 3262021SYJ001).