Evaluation of different attacks on Knowledge Based Authentication technique

Dr. Vijeet Meshram[1†]

Dr. Ambedkar College, Deekshabhoomi,
Nagpur, Maharashtra

Abstract
Knowledge Based Authentication is the most well-known technique for user authentication in a computer security framework. Most frameworks utilize a straightforward PIN (Personal Identification Number) or psssword as an data authenticator. Since password based authenticators typically will be software based, they are inclined to different attacks and weaknesses, from both human and software.Some of the attacks are talked about in this paper.

Keywords:
Authentication, Passwords, Security, Dictionary Attack, Mangling.

1. Introduction

Despite the fact that much has been said with regards to their shortcomings, passwords actually are and will be in the foreseeable future ubiquitous in authentication frameworks for Internet applications. They have an inherent tradeoff between convenience and security: as solid passwords are challenging for assailants to sort out, they are on the other hand moreover difficult for the client to remember.

So when researcher are discussing the frameworks that utilize passwords as an authentication scheme, it is subsequently fundamental to appropriately assess their adaptability to guessing attacks: which is done by comparing search space size against the percentage of passwords that would be broken by such an attack. This action doesn't rely upon the specific idea of the authentication framework nor on the attackers capacities: it is simply connected with the attack method and to the manner in which clients pick their password. The attack model and the attributes of the framework will rather characterize the expense that the attacker needs to pay for each single guess. By joining this cost with a proportion of the inquiry space, it becomes possible to acquire a sound cost saving advantage analysis for attacks in light of password speculating on an authentication system.

Manuscript received April 5, 2023
Manuscript revised April 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.4.14

2. Datasets Used

IT: The "Italian" dataset: This dataset contains the unencrypted passwords for the enrolled clients of an Italian instant messaging server taking on the XMPP convention, regulated by one of the creators. Researcher's investigation just reveals total data about the passwords of clients, and really establishes a piece of a security review of the framework. Storing passwords in plain text on the server is required by authentication algorithms like CRAM-MD5.
FI: The "Finnish" dataset: This dataset comes from a rundown of passwords that were openly unveiled in October 2007 by an unknown group. The list contained both unencrypted passwords and hashed (MD5); mostly from different Finnish web forums. The investigation was restricted to the unencrypted disclosed passwords.

MS: The MySpace dataset: A fake MySpace login page was made and afterward these passwords were acquired by the method for directing phishing attacks on that counterfeit MySpace login page, and were unveiled in October 2006 [1], [2]. Usernames, in this case, are email addresses. While this is one of the biggest dataset researcher is breaking down, there are a few inadequacies with it: initial one being that the researcher just has the passwords of clients who are less security cognisant and succumbed to the assault; second, clients might have (intentionally or unintentionally) set wrong passwords on their phishing page. MySpace login page was planned so the clients should embed both non-alphabetic and alphabetic characters in their passwords; and this forced a counterfeit effect on passwords that clients, left alone, would pick. By examining the distinctions between this dataset and the past ones, researcher can

assess the impact of this prerequisite on password strength.

Dataset	Size	#unique	Avg. length	#characters
IT	9,317	7,848	7.86	124
FI	15,812	13,395	7.60	90
MS	33,671	30,690	8.10	96

Table - 1.1. Summary information about datasets.

Table 1.1. Sums up a few data about researcher's datasets. It's intriguing to note that during all examples a couple of clients share the identical password. This could be a result of coincidence and use of too common passwords, however this could be also because of similar people enlisting under various usernames at a similar server. The normal password length is near eight in all cases, and the wide variety of utilized characters is better in IT because of the way that inconsistent Unicode characters were permitted, and utilized sparingly via the users.

Table - 1.2. Percentage of passwords matching various regular expressions.

Expression	Example	IT	FI	MS
[a-z]+	abcdef	51.21%	53.06%	1.09%
[A-Z]+	ABCDEF	0.29%	0.17%	0%
[A-Za-z]+	AbCdEf	53.74%	54.04%	1.09%
[0-9]+	123456	9.10%	3.43%	0.15%
[a-zA-Z0-9]+	A1b2C3	93.43%	95.43%	90.43%
[a-z]+[0-9]+	abc123	14.51%	27.10%	77.39%
[a-z]+1	abcde1	0.26%	1.43%	19.89%
[a-zA-Z]+[0-9]+	aBc123	16.30%	28.03%	77.48%
[0-9]+[a-zA-Z]+	123aBc	1.80%	2.16%	5.76%
[0-9]+[a-z]+	123abc	1.65%	2.09%	5.75%

In Table 1.2. Researcher looks at the matching ratio of various regular expressions in researcher's datasets. In all occasions, non-alphanumeric characters are available in just under 10% of the passwords. It is extremely intriguing to assess its matching proportions (with no strength authorization measures) with MS (where a mix of alphabetic and non-alphabetic characters is required). In MS, a small range of all-alphabetic or all-numeric passwords are available, and this could be a result of clients coincidentally or intentionally putting incorrect passwords in the phishing site page.

As already observed through Sebastian Porst [2], most MySpace clients notice the necessity of putting a non-alphabetic character via annexing a variety of toward the end of the password-kind of 20% of the clients unquestionably agree through including a "1". The impact of this action on password strength may moreover appear to be very dubious, explicitly for the situation that the attacker knows about the requirements.

A few clients in IT seem to have a more intense inclination toward settling on more grounded passwords with less effectively noticeable shape: as researcher will show in the accompanying, the complicated passwords from that dataset are the most troublesome ones to break.

3. Evaluation of attacks

3.1. Dictionary Attack

Dictionary attack is the least complex way to deal with the weakest passwords. Researcher took on the widely recognised and accessible tool called John the Ripper (JtR) password recovery tool. The prolonged dictionaries that specialists use are accessible for paid download from this tools website.

The Dictionaries: The JtR dictionaries include words from 21 distinct human dialects, in addition to a rundown of routinely utilized passwords. For a couple of dialects (like English and Italian), different word references of different sizes are available: the more modest ones incorporate just the most frequently utilized words while the greater ones additionally contain more noteworthy obscure words, the reasoning being that more typical expressions are significantly more liable to be chosen as passwords.

Taken by and large, all dictionaries represent right around 4 million words.
A recognised technique to make robust, however simple to recall passwords, is to transform phrases into passwords through removing an abbreviation, perhaps at the same time utilizing punctuation. For instance, the expression "Unfortunately, poor Yorick! I knew him, Horatio" becomes "A,pY!Ikh,H". Specialists furthermore assessed such abbreviations with a dictionary made through Kuo et al. [3] that was assembled through scraping sites showing memorable terms, including references and music verses.

Table - 1.3. Dictionary Attacks

Dictionary (size)	IT		FI	
	Found	Guess pr.	Found	Guess pr.
Frequent (2.8K)	5.95%	2.10E-05	2.86%	1.00E-05
English 1 lc (27K)	4.91%	1.80E-06	3.38%	1.20E-06
English 2 lc (297K)	9.42%	3.20E-07	6.26%	2.10E-07
English 3 lc (390K)	11.59%	3.00E-07	7.53%	1.90E-07
Extra lc (445K)	8.03%	1.80E-07	8.16%	1.80E-07
Italian 1 lc (63K)	3.71%	5.90E-07	0.79%	1.30E-07
Italian 2 lc (344K)	14.89%	4.30E-07	6.62%	1.90E-07
Finnish lc (359K)	8.45%	2.40E-07	20.24%	5.60E-07
All above (1.45M)	24.79%	1.70E-07	26.02%	1.80E-07
All JtR dicts (3.9M)	25.94%	6.60E-08	26.97%	6.60E-08
Mnemonics (406K)	1.27%	3.10E-08	0.35%	8.70E-09

3.2. Mangling

Numerous users take on simple strategies to guard passwords against dictionary attacks. A few examples are juxtaposition of words, attaching or prepending sequences of digits or symbols to passwords, or capitalizing words. The strategy of mangling is directed towards this objective: new applicant passwords are produced by rules modifying dictionary words. John the Ripper can utilize mangling rules to create an expanded set of passwords; specialists applied them to the "all dictionaries" list (3.9 million components) to produce a mangled rundown of 147,945,837 applicant passwords. With the lengthy dictionary depicted in the previous area, JtR moreover sends a hand-tuned dictionary containing 40,532,676 candidates - mangling strategies are chosen depending on the dictionary, with an alternate number of guidelines applied to each dictionary . This smaller dictionary is certifiably not a legitimate subset of the first, and contains a few words that can't be produced utilizing the default rules of JtR.
Probabilistic Context-Free Grammars: Recently, Weir et al. proposed another methodology for dictionary mangling based absolutely upon probabilistic context free grammars (PCFGs) [4]. In accordance with this technique, a probabilistic model is obtained from a preparation set of clear-text passwords, in steps. In the first place, the "structure" of the password is received and mapped to a context-free grammar production: for example, the "$abc123" password maps to the
S → S1 L3 D3 production (S is the starting non-terminal), addressing a series of one symbol, 3 letters, and 3 digits; the production is assigned a probability equivalent to its frequency inside the training set. The Li productions are made basically founded on the words from the dictionary to be mangled, simultaneously as the Si and Di creations are acquired, once more, from the training set: for example, if the D3 → 123 production is assigned a probability 0.4, and that implies 40% of all arrangements of 3 digits inside the dataset compare to the string "123".
This approach makes it conceivable to make a set of candidate passwords, and to assign a likelihood to every single one of them. In their work, Weir et al. planned an effective calculation to return an inconsistent number of creations through diminishing requests of likelihood.

Experimental Setup: Researcher made a training set from every one of researchers datasets, haphazardly picking half of the passwords in every one of them. Researcher then, at that point, utilized each training set to make three PCFG dictionaries mangling the "all languages" dictionaries of JtR, with distinct sizes. To permit smooth correlation with dictionary attack and the two JtR mangled dictionaries,

researcher chose the resulting sizes: 1.45 million, to match the "all above" line in table 1.3.; 40.5 million and 147.9 million to match the JtR dictionaries. Researcher then, at that point, mimicked a dictionary attack utilizing the nine dictionaries produced, in addition to the two JtR dictionaries , against 3 datasets. While considering a PCFG dictionary in contrast to the dataset from which the researcher obtained the training set, researcher just utilized half of the passwords that were not a piece of the training set.
Since the MySpace passwords ought to contain alphabetic and non-alphabetic characters, it is trivial for an attacker to utilize candidates that don't fulfill this essential. Researcher subsequently viewed it as an attack where those passwords have been sifted through from the mangled dictionary. Little amounts of additional passwords are seen when the algorithm is run utilizing the non-filtered dictionary: this is a result of the passwords in MS that don't consent to the security prerequisites of MySpace, as stated in Datasets.

Table - 1.4. Dictionary attacks with mangling techniques and probabilistic context-free grammars (pcfgs).

Dictionary (training set) (size)	IT		FI		MS (no filter)		MS (filtered dictionary)		
	Found	Guess pr.	Found	Guess pr.	Found	Guess pr.	Found	Guess pr.	Filtered dict size
PCFG (IT) (1.45M)	24.64%	1.7E-07	24.35%	0.00000017	0.90%	6.20E-09	0.21%	1.30E-07	17,015
PCFG (FI) (1.45M)	23.47%	1.60E-07	24.43%	0.00000017	0.75%	5.20E-09	0.06%	6.90E-08	9,413
PCFG (MS) (1.45M)	2.14%	1.50E-08	2.44%	1.7E-08	13.02%	9.00E-08	12.98%	9.00E-08	14,47,290
JtR hand-tuned (41M)	30.11%	7.40E-09	31.29%	7.70E-09	31.77%	7.80E-09	31.02%	1.00E-08	3,02,58,334
PCFG (IT) (41M)	30.88%	7.60E-09	36.17%	8.90E-09	30.93%	7.60E-09	30.22%	8.10E-09	3,71,14,836
PCFG (FI) (41M)	29.53%	7.30E-09	41.13%	1.00E-08	32.88%	8.10E-09	32.16%	8.80E-09	3,67,09,144
PCFG (MS) (41M)	20.88%	5.20E-09	28.97%	7.10E-09	38.52%	9.50E-09	37.88%	9.50E-09	3,96,74,064
JtR mangled (148M)	29.56%	2.00E-09	31.53%	2.10E-09	24.16%	1.60E-09	23.41%	2.20E-09	10,50,29,406
PCFG (IT) (148M)	33.12%	2.20E-09	41.81%	2.80E-09	43.62%	2.90E-09	42.90%	3.00E-09	14,43,23,223
PCFG (FI) (148M)	31.52%	2.10E-09	44.21%	3.00E-09	42.14%	2.80E-09	41.41%	2.90E-09	14,06,73,878
PCFG (MS) (148M)	30.28%	2.00E-09	41.18%	2.80E-09	48.27%	3.30E-09	47.46%	3.30E-09	14,54,80,767

4. Conclusion

In this work we zeroed in on the empirical investigation of real world passwords from three datasets, different as far as both application space and client localisation. We executed and involved an assortment of best in class procedures for password guessing, including dictionary attacks, mangling utilizing dictionaries and probabilistic context free grammars, and Markov chain-based systems. We proposed a special and far reaching analysis of the password strength of Internet applications. We estimated the flexibility of passwords as far as the search space expected for an attacker to figure a fraction of the portion of the passwords contained in our dataset and we concentrated on the properties of the different attack strategies we carried out. Our outcomes uncovered that no single attack system beats the others: dictionary attacks are best in finding weak passwords; dictionary mangling is valuable when the base dictionaries are depleted; Markov-chain strategies are strong in breaking strong passwords. All the attack strategies that we dissected are impacted by consistent losses: the likelihood to figure a password at each endeavor diminishes generally dramatically as the size of the investigated search space grows. Hence, the likelihood of achievement, eventually, won't justify anymore the expense for an attacker. Our outcomes can assist with tracking down this point. Our outcomes additionally shed light on certain parts of user practices in picking their passwords: we saw that as, inside our datasets, clients put moderately little exertion in picking their password when contrasted with the decision of their usernames. As shown by MySpace, embracing prohibitive password policies doesn't really forestall the formation of weak passwords. We accept that proactive password checkers are a superior methodology, and we are at present carrying out one such instrument in light of the discoveries of this work: given at least one assault model, it will compute in real time an estimate of the quantity of guesses expected to break the password. This data will be given to the client as an estimate of password strength. Our future exploration plan will likewise zero in on client conduct in view of information we are at present gathering on the Internet: we are specifically keen on surveying the connection,

if any, between password strength, user activity levels, and the application domain.

References

1. R.A.Grimes, “My Space password exploit : Crunching the numbers (and letters),” InfoWorld online article, November 2006. [Online]. Available: http://www.infoworld.com/article/06/11/17/47OPsecadvise_1.html
2. S. Porst, “A brief analysis of 40,000 leaked MySpace passwords,” Blog post, November 2007. [Online]. Available: http://www.the-interweb.com/serendipity/index.php?/archives/94-A-brief-analysis-of-40,000-leaked-MySpace-passwords.htm
3. C.Kuo,S.Romanosky,andL.F.Cranor,“Human selection of mnemonic phrase-based passwords,” in *Proc. SOUPS ’06*, 2006, pp. 67–78.
4. M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, “Password cracking using probabilistic context-free grammars,” in *IEEE Symposium on Security and Privacy*. IEEE, May 2009, pp. 391–405.

Dr. Vijeet Meshram received doctorate degree in 2021 and his area of interests are security and authentication, he has been teaching post graduate students in the department of computer science in Dr. Ambedkar college, Nagpur, India from 2015. He is affiliated with the university and sets question papers and designs curriculum for students.