Learning Framework for Guessing Alphanumeric Passwords on Mobile Phones Based on User Context and Fragment Semantics

Lilian Noronha Nassif[1,2(✉)] and Jonny Silva de Oliveira[1]

[1] Public Ministry of Minas Gerais State, Av. Álvares Cabral, 1690, Belo Horizonte, Brazil
{liliannassif,jsoliveira.plansul}@mpmg.mp.br
[2] Pontifical Catholic University of Minas Gerais, Av. Dom José Gaspar, 500, Belo Horizonte, Brazil

Abstract. When conducting a criminal investigation, accessing mobile phone data is crucial for law enforcement. However, encryption mechanisms and user locks are becoming increasingly complex and more challenging for forensic examiners. Although there are tools that can perform brute-force attacks to crack passwords on mobile phones, it becomes difficult when faced with alphanumeric passwords. The challenge is not only the algorithm but also the use of a customized dictionary. It is impractical to use a complete dictionary with all possible combinations as the attack conditions are very restrictive, and the time it takes to crack the password becomes too long depending on its length. In this article, we present a learning framework based on a set of dictionaries, variation rules, and fragment permutations. Dictionaries are organized from different perspectives of personal data, open sources, and groups of contexts. The naming and ordering of the dictionary help digital forensics examiners strategize and improve their chances of success in cracking alphanumeric passwords.

Keywords: Digital Forensics · Password Guessing · Mobile Forensics

1 Introduction

The branch of forensic science that deals with mobile devices, known as mobile forensics, has become increasingly relevant for criminal investigations. With the widespread use of digital devices for daily activities, as well as the advancements in computational power, storage, and memory, there is a vast amount of data that can be recorded [1]. However, there are also technologies in place to protect information privacy, such as encryption and access blocking.

One of the main obstacles that forensic examiners face when dealing with a locked mobile phone is confirming that it is secured with an alphanumeric password. The digital forensics industry has already managed to overcome the challenge of breaking codes for mobile phones locked with numeric passwords or pattern codes by utilizing a brute force technique. This involves making exhaustive attempts to try out all possible combinations,

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2024
Published by Springer Nature Switzerland AG 2024. All Rights Reserved
S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 571, pp. 23–30, 2024.
https://doi.org/10.1007/978-3-031-56583-0_2

with the expectation of obtaining the correct password within a timeframe ranging from a few hours to a maximum of one year.

However, when it comes to alphanumeric passwords, a single dictionary is often not sufficient and the password length is unknown. The challenge in this scenario is not with the algorithm or device access, but in constructing a comprehensive dictionary of potential passwords.

In this work, we introduce a framework that enables the creation of dictionaries from various data sources. The framework involves applying modification rules and rearranging fragment positions. The data sources used in this approach include intelligence activities, digital forensics expertise, and research of generic and specific wordlists. Additionally, the framework allows for the incorporation of machine learning techniques.

The structure of this paper is as follows: Sect. 2 provides information on related works. Section 3 lays out the structured phases for creating and enhancing cracking dictionaries. Section 4 covers the implementation of the framework. Finally, Sect. 5 concludes the paper.

2 Related Works

In the literature, two main approaches are used to gain insight into how users create their own passwords. The first approach involves analyzing leaked password databases to present statistics on password length, data type correlation, and semantic analysis. The second approach involves conducting surveys with volunteer groups to ask about their password creation strategies.

In their study, Kanta et al. [2] examined the HIBP_v5 database which contained 3.9 billion accounts. The analysis examined usage statistics and identified the most common patterns in passwords, including fragments based on their semantic meaning.

According to the findings of Brown et al. [3], two-thirds of people create passwords using their personal data. The remaining one-third mostly uses personal data of their relatives, friends, or significant others. The most commonly used information for passwords is first names and birthdays. Shockingly, almost all respondents reuse passwords on different sites or devices. Additionally, about two-thirds of passwords are duplicates.

The work of Hunt [4], reveals that 14% of passwords derive from a first name and most people add numbers after words, usually 2 or 4 numbers, suggesting they are fragments of birthday dates. Hunt also describes that 8% of the analyzed passwords use place names. Dictionary words appeared in 25% of the analyzed passwords. He also identified that 14% of passwords are purely numerical, not having any other type of character. The length of purely numeric passwords were identified as follows: 4-digit passwords (8%); 6-digit passwords (48%); 8-digit pass-words (27%); other length passwords (17%). It is possible to realized that even password lengths are more frequent than odd passwords lengths. Hunt also analyzed that 2.7% of passwords repeated words, such as: “lovelove”; another 2.6% use email login as their password. It was also detected that 1.3% of the passwords use short phrases, such as “Iloveyou”; and 0.3% use keyboard patterns such as “qwerty”. The remaining 31% of the analyzed passwords were not related to any pattern.

3 Structured Phases of Guessing Passwords

3.1 Data Sources for Customized Dictionaries

Various methods can be used to gather data sources for creating dictionaries for password attacks. These include investigation, research in open sources, digital forensics examination of devices belonging to the target, selecting wordlists based on themes, and using password generation programs.

Table 1 provides a taxonomy that categorizes data sources based on their origin, and includes examples of information and the corresponding dictionary name (DICX.Y) created from that source. The X refers to group identification and Y refers to group subset.

Table 1. Taxonomy of data sources for customizing dictionaries

Data sources	Category	Examples	Dictionary
Case investigators	Personal data	Name, date of birth, name of relatives and friends	DIC1
Digital evidence to attack (extraction BFU – Before First Unlock)	Digital forensics	e-mail, user name	DIC2
Other digital evidence of the same person or online credentials	Digital forensics	Words used in communications	DIC3
OSINT (Internet)	Open sources	Cities and places visited, friends, important dates, musical preferences, political preferences	DIC4
Generic searches of ready-made dictionaries (Internet)	Related word groups	People name dictionaries, animal name dictionaries, city name dictionaries, football team name dictionaries	DIC5.Y
Developed by the authors	Password generation program	Numbers, letters and special characters 4, 5, 6, 7, 8, 9	DIC6.Y
Leaked password dictionaries (Internet)	Hacker community	Rockyou, HIBP (Have I Been Pwned?), MySpace	DIC7.Y
Researched/elaborated by the authors	Short sentences	Short and common phrases: “IloveYou”, “goodblessyou”, “verygood”	DIC8
Researched/elaborated by the authors	Long sentences	Song initials, use of popular long phrase initials	DIC9

The dictionary named DIC1 is created from information provided by the investigator to the forensic examiner. This dictionary is based on the high likelihood of the target using personal information when creating passwords. Table 1 organizes dictionaries in order of personal to generic data and from simple to complex passwords.

The BFU data source, used to compile the DIC2 dictionary, extracts data from mobile phones before the first unlock. This includes information from the operating system, as well as mobile phone username, email [5], and cloud data access credentials login accounts. Researchers can explore this data in open data sources (OSINT), facilitated by various applications listed in Bielska's document [6]. DIC4 is a dictionary created from OSINT data sources which reveal target's habits, tastes, and relationships, such as preferences for sports teams, political and religious affiliations, and hobbies [7]. DIC5 contains specific groups related to hobbies, such as motorcycling, with subgroups containing all words, slang, brands, and models of motorcycles. Quick & Choo [8] refer to this correlation between OSINT and intelligence in digital forensics as DFINT.

Another strategy to guess passwords is to examine other electronic devices seized from the same target, such as notebooks with less complex passwords. This strategy can generate DIC3, a dictionary containing a wordlist ordered by the most frequent words and a profile analysis of the target's habits. Bang et al. [9] found that 80% of users keep their passwords, 16% use a password already used on another site, and only 4% change their password completely when creating a new one.

Thus, the data sources that form DIC1 to DIC5 dictionaries have interrelationships, as shown in Fig. 1. Analysis of DIC1 to DIC4 can be used to create DIC5 wordlists associated with hobbies, trips, favorite sports, and more.

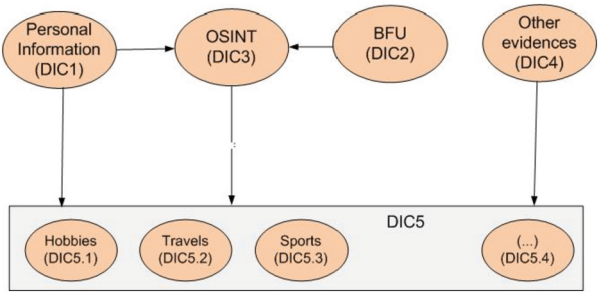

Fig. 1. Intercorrelation among dictionaries DIC1 to DIC5.

The dictionaries DIC6, DIC7, DIC8, and DIC9 listed in Table 1 are created using generic sources and do not contain any information specific to the target. DIC6 includes all possible word constructions, making it appear to be the most straightforward method to crack passwords by trying all combinations of letters, numbers, and special characters for all password lengths. However, as we will explain in Sect. 3.3, brute force attacks on locked mobile phones would only be effective for passwords up to 4 characters long.

3.2 Time to Crack Alphanumeric Passwords on Mobile Phones

Digital forensics tools often install agents with dictionary size limitations for cracking passwords on mobile phones. For Android phones, attacks are limited to files of 200 MB, while for iPhones, it is 15 MB. This means that every time a dictionary is exhausted, the device must be reconnected and the dictionary changed.

Studies have shown that internet passwords can be cracked within 8 h, but this is not the case for agents installed on locked mobile phones with alphanumeric passwords [10]. The processing power and conditions are much more restricted, leading to slower attacks with only a few thousand attempts per minute. Additionally, the forensic examiner must manually disconnect and change the dictionary every time it is exhausted.

For instance, if using DIC5 with 4 characters in Table 1, 3 files are used for Androids and 33 files are used for iPhones. This means that the forensic examiner would have to wait for each dictionary to be exhausted before selecting another one and reconnecting cables up to 33 times in the worst-case scenario. If the password length is 5 characters (with 26 letters, 10 numbers, and 7 special characters), this becomes even more impractical, requiring 3611 manual dictionary changes for iPhones. Therefore, brute-force methods become impractical for passwords with 5 digits and above, which is why this paper presents mechanisms to improve password guessing.

3.3 Variations in the Dictionary

Based on the data sources provided in Sect. 3.1, it is still possible to alter the dictionary by making mutations using special characters, modifying the position of capital letters, adding numbers, and utilizing acronyms.

These variations are typical human behaviors when creating passwords, such as adding a digit at the end, capitalizing the first letter, and replacing letters with similar symbols (@ for “a”, 3 for “E”, and 1 for “i”).

Table 2. Variations in dictionaries according to predictable human behavior.

Variation Name	Description	Variation ID
Special character replacement	Replace “E” with “3”, “i” with “1”, “a” with “@”, “o” with “0”	VAR1
Changing the position of the capital letter	Change capitalization in all positions where there are letters	VAR2
Addition of numbers	Add 2 to 4 numbers	VAR3
Use initial letters of words	Compose words using sentence and full names initials	VAR4

3.4 Personal Data Decomposition and Fragment Permutation

Creating a strong password can be made easier by breaking down personal data into separate parts. All personal information, including that of a person’s relatives, friends

and romantic partners, is important. Here are some examples of how to break down personal data: 1) For each birthday, it is important to separate the day, month, year, and full year in reverse order (dD, mM, yY, and yyYY); 2) For a full name, consider each word separately, including the initials; 3) For documents with numbers, separate them into groups of 3 and 4 numbers, as well as the complete number. This breakdown of personal data is also discussed in [11], which classifies birth dates, usernames, telephone numbers, emails, and other personal data as a semantic category of the password.

In addition to breaking down personal data, it is also important to identify common groups of fragments when creating a password. Typically, people start a sentence with a capital letter and end it with a punctuation mark. Therefore, a stronger password could be composed of three fragments: Fragment1 - a word or initials with the first letter capitalized (using words from dictionaries such as DIC5, 7, 8, 9); Fragment2 - numbers associated with dates or personal documents (Dd, Mm, Yy) or (dD, mM, yY) or (DdMm) or (YYYY); Fragment3 - special characters (&, *, $, #, @, %, !, ?) with variations of combination or repetition of the same special character (Fig. 2).

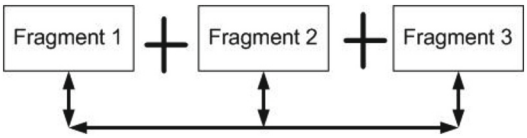

Fig. 2. Semantics of passwords by fragments.

Although the proposed fragment order (Fragment 1 + Fragment 2 + Fragment 3) are the most common rule, it is also important permutate each fragment position to create more password guessing possibilities.

Although the recommended order for fragments is usually Fragment 1 + Fragment 2 + Fragment 3, it is crucial to permute the position of each fragment to increase the number of possible password guesses.

4 Implementation of the Framework Model

The framework model was implemented through a series of steps outlined in Sect. 3. The authors developed a program to execute each step, which are summarized below:

1. Researching the data source
2. Breaking down personal data into each piece of information for the target and their relationships
3. Creating dictionaries for each data source (DIC1 to DIC9 in Table 1)
4. Creating variations for each dictionary (VAR1 to VAR4 in Table 2)
5. Changing the position of fragments for each DICx-y-VARx
6. Analyzing the semantics of cracked passwords and improving dictionaries through machine learning.

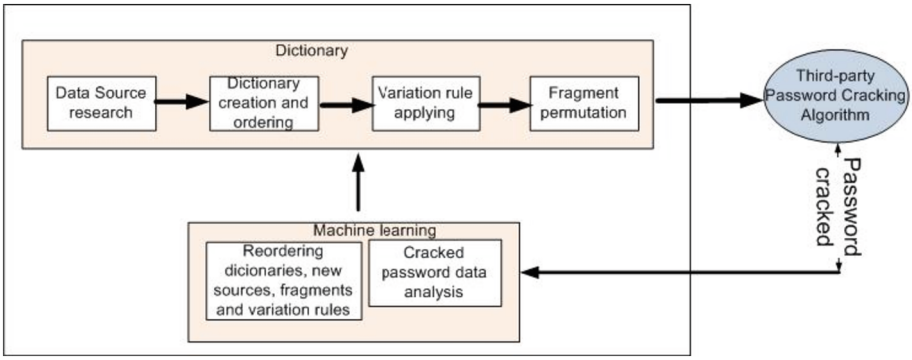

Fig. 3. Learning framework for guessing alphanumeric passwords

These steps were all successfully implemented, resulting in a comprehensive and efficient framework model.

Figure 3 presents the full framework of our solution. The creation of effective dictionaries for use in a third-party password cracking algorithm involves well-defined stages. The framework's mechanisms can be refined and customized through machine learning with additional real-world examples.

5 Conclusion

Cracking alphanumeric passwords on mobile devices during investigations has proven to be a challenging task for law enforcement. While a brute force attack can crack a password up to 9 characters in a few weeks, the scenario is different when it comes to cracking alphanumeric passwords on mobile phones. Digital forensics solutions install an agent on the device, which limits the dictionary size and processor performance. This size limitation requires forensic examiners to manually make changes to the dictionary, wasting precious time. Therefore, brute force is not feasible when the number of changes is large, that is, over or equal to 5 alphanumeric character combinations.

To overcome this challenge, this article presents the best dictionary assembly strategies that carefully select words and numbers related to the user's context. The article also includes necessary variations on the assembled dictionaries and permutations of fragment positions.

The learning framework for cracking alphanumeric passwords was able to organize the work within the forensic laboratory. This demonstrated the limitations of brute force and included intelligence in the dictionary's assembly. All dictionaries were named and organized to establish the correct preparations and sequence of use for each new mobile phone with an alphanumeric password to be cracked in the digital forensic laboratory.

References

1. Sathe, S.C., Dongre, N.M.: Data acquisition techniques in mobile forensics. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, pp. 280–286 (2018). https://doi.org/10.1109/ICISC.2018.8399079

2. Kanta, A., Coray, S., Coisel, I., Scanlon, M.: How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts. Forensic Sci. Int.: Digit. Invest. **37** (2021)
3. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K.: Generating and remembering passwords. Appl. Cognit. Psychol.: Off. J. Soc. Appl. Res. Mem. Cogn. **18**(6), 641–651 (2004)
4. Hunt, T.: The science of password selections. TroyHunt.com blog (2011). https://www.troyhunt.com/science-of-password-selection/
5. Fukami, A., Stoykova, R., Geradts, Z.: A new model for forensic data extraction from encrypted mobile devices. Forensic Sci. Int.: Digit. Invest. **38**, 301169 (2021). https://doi.org/10.1016/j.fsidi.2021.301169. ISSN 2666-2817
6. Bielska, A., Kurs, N., Baumgartner, Y., Benetis, V.: OpenSource intelligence tools and resources handbook. I-Intelligence (2020). https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf
7. Kanta, A., Coisel, I., Scanlon, M.: A survey exploring open source intelligence for smarter password cracking. Forensic Sci. Int.: Digit. Invest. **35**, 301075 (2020). https://doi.org/10.1016/j.fsidi.2020.301075
8. Quick, D., Choo, K.: Digital forensic intelligence: data subsets and open source intelligence (DFINT+OSINT): a timely and cohesive mix. Future Gener. Comput. Syst. **78**(Part 2), 558–567 (2018). https://doi.org/10.1016/j.future.2016.12.032. ISSN 0167-739X
9. Bang, Y., Lee, D., Bae, Y., Ahn, J.: Improving information security management: an analysis of ID–password usage and a new login vulnerability measure. Int. J. Inf. Manage. **32**(5), 409–418 (2012). https://doi.org/10.1016/j.ijinfomgt.2012.01.001. ISSN 0268-4012
10. Vo, N.: How long does it take to crack a password? A brief explanation. Locker (2022). https://locker.io/blog/time-to-crack-a-password
11. Jiang, X., Sun, X., Liu, Q.: Password guessing attack based on probabilistic context free algorithm. In: 2022 IEEE 8th International Conference on Computer and Communications (ICCC), Chengdu, China, pp. 1234–1238 (2022). https://doi.org/10.1109/ICCC56324.2022.10065766