

Password Cracking and Countermeasures in Computer Security: A Survey

Aaron L.-F. Han^{*^}

Derek F. Wong^{*}

Lidia S. Chao^{*}

^{*} *NLP²CT* Lab, University of Macau, Macau SAR

[^] ILLC, University of Amsterdam, Science Park 107, 1098 XG Amsterdam

l.han@uva.nl

derekw@umac.mo

lidiasc@umac.mo

Abstract—With the rapid development of internet technologies, social networks, and other related areas, user authentication becomes more and more important to protect the data of the users. Password authentication is one of the widely used methods to achieve authentication for legal users and defense against intruders. There have been many password cracking methods developed during the past years, and people have been designing the countermeasures against password cracking all the time. However, we find that the survey work on the password cracking research has not been done very much. This paper is mainly to give a brief review of the password cracking methods, import technologies of password cracking, and the countermeasures against password cracking that are usually designed at two stages including the password design stage (e.g. user education, dynamic password, use of tokens, computer generations) and after the design (e.g. reactive password checking, proactive password checking, password encryption, access control). The main objective of this work is offering the abecedarian IT security professionals and the common audiences with some knowledge about the computer security and password cracking, and promoting the development of this area.

Keywords- *Computer security; User authentication; Password cracking; Cryptanalysis; Countermeasures*

I. INTRODUCTION

The password has been used to encrypt the information or message for a long time in the history and it leads to a discipline: cryptography [1]. Furthermore, with the rapid development of computer science, the password is now also commonly used for the user authentication issue, which is very important to the internet security [2] [3].

RFC 2828 defines user authentication as “the process of verifying an identity claimed by or for a system entity”. The authentication service must assure that the connection is not interfered with by a third party masquerading as one of the two legitimate parties, which usually concerns two approaches data origin authentication and peer entity authentication [4]. The data origin authentication provides for the corroboration of the source of a data unit without the protection against the duplication or modification of data units, and this type of service supports applications like email where there are no prior interactions between the

communicating entities. The peer entity authentication provides for the corroboration of the identity of a peer entity in an association for use of a connection at the establishment or at times during the data transfer phase, which attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

There are usually four means of authenticating user identity based on: something the individual knows (e.g. password, PIN, answers to prearranged questions), something the individual possesses (token, e.g. smartcard, electronic keycard, physical key), something the individual is (static biometrics, e.g. fingerprint, retina, face), and something the individual does (dynamic biometrics, e.g. voice pattern, handwriting, typing rhythm) [5][6][4]. In the different methods, password authentication (something the individual knows) is widely used line of defense against intruders [7]. In the password authentication scheme, user ID determines that the user is authorized to access the system and the user’s privileges. It is also sometimes used in discretionary access control meaning that others can login using your identity. When user provides name/login and password the system compares password with the one stored for that specified login. However, some users do not pay attention to the confidentiality or complexity of their passwords thinking that they do not have any private files on the internet. This allows the malicious crackers to make the damage on the entire system if they provide an entry point to the system [8]. Furthermore, the higher speed computational processors have made the threats of system crackers, data theft and data corruption easier than before [9].

This paper is constructed as below: Section 2 introduces the related work about computer security and password cracking; Section 3 introduces the password application in remote user authentication and the vulnerabilities; Section 4 presents the password cracking methods including traditional methods and the import technologies from other literatures such as mathematics and linguistics; Section 5 presents the countermeasures for password cracking and Section 6 shows the conclusions closely followed with appendix of available software.

II. RELATED WORKS

Morris and Thompson [10] conduct a brief case study of the password security and specify that the salted passwords (12-bit random quantity) are less predictable at that time. Jobusch and Oldehoeft [11][12] show that password mechanisms remain the predominant method of identifying computer system users. They first give a review of the authentication, discuss the vulnerabilities of password mechanisms at that time, and then describe an extension of the UNIX password system with the permission of the use of pass-phrases. Spafford [13][14] designs a sufficiently complex password screening dictionary OPUS to prevent weak password choices with a space-efficient method. Cazier and Medlin [15] present a research of the password security and the password cracking time focusing on the e-commerce passwords. Their empirical investigation shows that e-commerce users usually create the passwords without guidance from the web site and they tend to create short or simple passwords such that they can easily remember them. Marechal [16] presents some existing hardware architectures of that time dedicated to password cracking, such as Field-programmable gate array (FPGAs) that are devices containing fully programmable logic and CELL processor (a core processor of the PlayStation3 console) that are developed by Sony, Toshiba and IBM. Snyder [17] designs a pattern for creating individualized learning exercises in the area of security education with password cracking/recovery realized in practice. Furnell [18] discusses the website password protection issues of three aspects including whether the sites provide any guidance when users select passwords, whether any restrictions are imposed on passwords, and whether offers means to help users who have forgotten the passwords. Plaga [19] conducts a research on the suitable use cases of the biometric keys. Winder [20] briefly introduces some of the mostly used password cracking methods including dictionary attack, brute-force attack, rainbow table attack, malware, offline cracking, and guessing, etc.

Other related works include that Bonneau [21] conducts an analyzing of anonymized corpus of 70 million passwords; Kelley et al. [22] measure the password strength by simulating password-cracking algorithms; Zhang et al. [23] introduce a time-memory-resource trade-off method for password recovery; Klein [24] describes a collection of attacks used by surfers and web sites against other web sites, as well as attacks by web sites against surfers; Houshmand and Aggarwal [25] introduce the probabilistic techniques to enhance the passwords.

Different from the previous works, this paper will give the discussions on both the password cracking methods and the countermeasures against password cracking. Furthermore, to read this paper, you need not any background knowledge. Thus, we hope it can offer the abecedarian IT security professionals and the common audiences with some knowledge about the computer security and password cracking, and promote the development of this area.

III. PASSWORD IN REMOTE USER AUTHENTICATION

In the remote user authentication, password protocol is used when the password is employed for authentication [2] [4]. In the password protocol scheme, user first transmits identity to remote host; then the host generates a random number (nonce) and the random number is returned to the user, at the same time host stores a hash code of the password; the user hashes the password with the random number (a random number helps defend against an adversary capturing the user's transmission) and sends it to the host; the host compares the stored information with the received one from the user to check whether they match or not. Remote user authentication is the authentication over a network, the internet, or a communications link. The additional security threats of remote user authentication include eavesdropping, capturing a password, replaying an authentication sequence that has been observed. Remote user authentication generally relies on some form of a challenge-response protocol to counter threats.

IV. PASSWORD CRACKING METHODS

A. Traditional Password Cracking Methods

Since passwords remain the most widely used mechanism to authenticate users, obtaining the passwords is still a common and effective attack approach [26]. The traditional password cracking methods include stealing, defrauding, user analysis, algorithm analysis and fully guessing, etc. which will be introduced below.

1) Stealing

Password stealing can be achieved by looking around the person's desk, shoulder surfing, sniffing the connection to the network to acquire unencrypted passwords, gaining access to a password database and malware. In the shoulder surfing, hackers will take the guise of a parcel courier, service technician or something else to make them get access to an office. After they get in the building, the service personnel uniform provides a kind of free pass to wander around and make note of passwords being entered by genuine members of staff [20]. In the malware attack, the key logger or screen scraper is usually installed by malware that can record everything the user type and take screen shots during the login process. Furthermore, some malwares try to look for the existence of a web browser client password file and copy the accessible passwords from the browsing history.

2) Defrauding

Another way to gain the password is to defraud the users by social engineering or phishing on line. Social engineering will take the jugglery in the real world. One case is to telephone an office pretending as a professional IT security technician and ask for the users' account (or network) access passwords [15]. In the phishing attack, users will receive a phishing email that contains links leading to faked websites such as the online banking and payment, etc. and makes some terrible problem to the accounts' security.

3) User Analysis

Users tend to generate the passwords based on the things they usually chat about on social networks or somewhere

TABLE I. AVERAGE TIME REQUIRED FOR EXHAUSTIVE KEY SEARCH [4]

Key size (bits)	Number of alternative keys	Time required at 1 Decryption/ μ s	Time required at 106 Decryptions/ μ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8 \text{ minutes}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142 \text{ years}$	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$	$5.4 \times 10^{18} \text{ years}$
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$	$5.9 \times 10^{30} \text{ years}$
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$	$6.4 \times 10^6 \text{ years}$

TABLE II. COMPARISON OF THREE POPULAR SYMMETRIC ENCRYPTION ALGORITHMS [4], DES: DATA ENCRYPTION STANDARD; AES: ADVANCED ENCRYPTION STANDARD

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

else. Password crackers are likely to look at this kind of information and make a few guesses during the cracking of passwords. The hackers can reduce the password cracking time by the analysis of the special users according to their characteristics, such as the persons’ name, job title, interests, families, hobbies, and so on. One of such kind of attack is known as Spidering. The hackers realize that many corporate passwords are generated by connecting to the business itself. They try to build custom word lists by the studying of corporate literature, website material and listed customers, etc.

4) *Algorithm Analysis*

Algorithm analysis attacks focus on the used encryption algorithms such as the cryptanalytic attacks which are also used in the decryption of ciphertext [9]. It relies on the nature of the algorithm, some knowledge of the general characteristics of the text and some sample of plaintext-ciphertext pairs. This kind of attack exploits the characteristics of the algorithms to attempt to deduce a specific plaintext or the keys.

5) *Fully Guessing*

The widely used kind of method for password cracking is the fully guessing include the dictionary attack, brute-force attack, hybrid of dictionary and brute-force [15], rainbow table attacks, etc.

In the dictionary attack, a large dictionary containing of possible passwords (commonly used passwords, e.g. the common dictionary words, the combination of several words the pun, etc.) is used by the hackers attempting to gain the access to the users’ computer or network [27]. The common approach is applying the same encryption method to the dictionary of passwords to compare with the copy of an encrypted file containing the passwords. If the encryption method has used the hash function, then each dictionary password must be hashed using each salt value to compare with the stored hash values. Berger et al. [28] also introduce the dictionary attacks using keyboard acoustic emanations.

Brute-force attack guesses the password using a random approach by trying different passwords and hoping one works [29]. This approach is different with the dictionary attack with the using of non-dictionary words, which can

contain all possible alpha-numeric even special character combinations, such as “aaaaa000”, “zzzzz9999” and “bbb&&99\$00”. If some logic analysis is employed in the brute-force attack the password cracking time may be reduced sometimes, e.g. the using of previously mentioned user analysis (using persons’ name, job information and hobbies). Assuming that the users’ passwords are over a handful of characters long, the brute-force attack can crack the passwords eventually even though it costs a lot of time. The use of distributed computing models and zombie botnets can short the cracking time. Brute-force attack is also used in the decryption of ciphertext where it tries all possible keys on the ciphertext until an intelligible translation output of plaintext is gained. As supplementary, the Table 1 and Table 2 show the example of the average time required for brute-force attack on the symmetric encryption and the key size of several popular symmetric encryption algorithms.

In the rainbow table attacks, the hackers use a rainbow table that is a list of pre-computed hash values for all encrypted passwords with all salts [30]. The time that rainbow table attack takes to crack a password is reduced to the time it takes to look it up in the list. This kind of attack could be countered by the use of a sufficiently large salt value and a sufficiently large hash length. Rainbow table attacks have been used widely, e.g. [31], [32] and MD5 online cracking using rainbow tables¹.

If the password cracking is conducted online, the protection system usually locks out the users after they failed to login the system for more than three times to block the automated guessing software. However, the offline attacks usually escape from this. In the offline attack, hackers first break into a system to steal the encrypted password files or eavesdrop on an encrypted exchange on the internet. Then the password cracker can take as long as they need to try and crack the code without alerting the target system or individual user.

¹ <http://www.passcracking.com/>

B. Import Technology of Other Literature

Some algorithms or models are imported from other literatures to be combined with the existing password cracking methodologies, such as the mathematical Markov model and the linguistic context-free grammar.

1) Markov Chains Based Method

Markov models are used in some of the password crackers or recovery tools, such as [33], [34], the John the Ripper² password cracker [35] and AccessData's Password Recovery Tool [36]. The Markov chains can reduce the search space which will be needed if the brute-force attack is used.

Narayanan and Shmatikov [33] use the Markovian filters to capture the phonetic similarity with words in the users' native languages (only seeking the "memorable" strings) and employ the finite automate model to deal with the non-alphabetic characters in the passwords. The used Markov models include zero-order model and first-order model. In the zero-order Markov model, characters are independent with each other and they are generated according to the probability distribution with the description formula (P is used for the Markovian probability, v as the frequency of the character):

$$P(\alpha) = \prod_{x \in \alpha} v(x) \quad (1)$$

On the other hand, the characters in the first-order Markov model are dependent and each character will be assigned a probability by looking at the previous characters (symbol "[|" representing that the right part is the premise of the left part):

$$P(x_1, x_2, \dots, x_n) = v(x_1) \prod_{i=1}^{n-1} v(x_{i+1}|x_i) \quad (2)$$

In their experiments, they test the approaches on the data of 150 user passwords and recover 67.6% coverage using a search space of size 2×10^9 compared with the Oechslin's attack [31] that achieves 27.5%. Marechal [16] presents that Markov chains can also be used as a powerful tool for improving distributed and rainbow table cracking.

C. Probabilistic Context-Free Grammars

Weir et al. [37] employ Probabilistic Context-Free Grammars (PCFG) for password cracking. They first create a probabilistic context-free grammar which is based on a training set of disclosed passwords. They incorporate the probability distribution information of user passwords to generate password patterns. They use the grammar to generate word-mangling rules which will be employed in the password guessing period with dictionary attack. The material they used include three word lists that are MySpace test list (containing 33481 plaintext words), SilentWhisper list (7480 plaintext passwords) and Finnish test list (22733 unique MD5 password hashes) and six input dictionaries, of which four dictionaries (English_lower, Finnish_lower, Swedish_lower and common_Passwords) are from John the

Ripper with other two dictionaries "dic-0294" (from a password-cracking site³) and "English_Wiki" (user updated dictionaries⁴). Their method has shown improvement of 28% to 129% as compared to a publicly available password cracking program "John the Ripper" testing on a set of disclosed passwords. The running time information is that it can generate 1144895.1 unhashed guesses per second using a computer that equipped with "MaxOSX 2.2GHz Intel Core 2 Duo". Rao et al. [38] also introduce a work about the effect of grammar on security of long passwords.

V. COUNTERMEASURES FOR PASSWORD CRACKING

The protecting of passwords from compromise and unauthorized use is a crucial issue since the passwords remain the most popular approach for authentication. The countermeasures for password cracking could be achieved in two stages generally, i.e. the password design stage and after the generation.

A. Password Design Stage

1) User Education

Users can be educated with the importance of using strong passwords and be trained how to generate hard to guess passwords using some password selection strategies. For instance, the password must contain letters (both capital Letters and small Letters), numbers, and special characters; the length of the password must not be less than a certain number; the use of passphrase which is usually longer than a word; the use of beginning characters of each word in a memorable sentence, etc. Shay et al. [39] emphasize the importance of user attitudes and behaviors for stronger passwords. Komanduri et al. [40] conduct a research to measure the effect of password-composition policies (e.g., requiring passwords to contain symbols and numbers), and explore the relationship between password-composition policies and the strength of the resulting passwords. They characterize the predictability of passwords by calculating the entropy and find that some commonly held beliefs about password composition and strength are inaccurate. They give a contribution by several recommendations for password-composition policies that result in strong passwords.

2) Dynamic Password

Cole [26] gives the introduction of the one-time password, dynamic password and static password, of which one-time password is one way to provide a high level of security. In a one-time password scheme, a new password is required each time when the user log on the account to prevent the hackers from using a pre-compromised password. The dynamic password specifies that the password is changed frequently or at a short time interval while the static password means the password is the same for all the time when logging on the system. The organization could force some requirements for the users to change the passwords periodically, e.g. weekly, monthly, or every half-year. The length of time interval can be based on the sensitivity of the

² <http://www.openwall.com/john/>

³ <http://www.outpost9.com/files/WordLists.html>

⁴ www.wiktionary.org

protected information. Zhang et al. [41] propose an algorithmic framework and empirical analysis about the security of modern password expiration.

3) *Use of Token*

The password can be generated using some security tokens that are used to ease authentication by authorized users of computer services. The token may be a physical device such as the smart cards (it may also refer to software token or virtual token). The password appearing on the token can be changed regularly with a time interval, which achieves the dynamic password mechanism and reduces the value of stolen passwords because of its short time validity. Furthermore, constantly shifting password reduces the probability of successful cracking by brute-force attack if the attacker uses the password list within a single shift. The challenge is how to deal with synchronicity of the token and the server due to the fact that there will be a time-delay before the password reaches the token from the server. After the user types in the password appearing on the token the password on the server site may be already changed to the next one due to the time delay. The token can be also equipped with inserted switch algorithms. In this case, the user types in the numbers appearing on the token then the calculator will generate a password using the inserted algorithms. Gyorffy et al. [42] propose a method of token-based graphical password authentication.

4) *Computer Generated Passwords*

Users can also use the computer generated password for their account. Using some pre-design, the computer generated password usually ensures a certain length, contains special characters and is un-pronounceable, which is difficult for the hackers to crack successfully within a short time. However, computer generated password is not easily to remember for the users due to the fact that it is mostly meaningless. Molloy and Li [43] introduce a work about the attack on the GridCode one-time password. Chiasson et al. [44] introduce the research on user interface design to affect security.

B. *After the Generation of Passwords*

1) *Reactive Password Checking*

In a reactive password checking strategy, the system periodically runs its own password cracker to find guessable passwords. The system will cancel passwords that are guessed and notifies the users. The disadvantages are that it consumes resources very much and the hackers can also use this strategy to find the weak passwords if they get the password file copy⁵. Weir et al. [45] introduce a research work about testing metrics for password creation policies by attacking large sets of revealed passwords.

2) *Proactive Password Checker*

Another way to reject the weak passwords is proactive password checking. Different with reactive password checking, proactive password checking allows users to select their own password [46]. However the system will check if the password is allowable or not. The goal is that users can

select memorable passwords that are difficult to guess. Many researchers have designed their proactive password checkers. For example, Klein [47] proposes a proactive password checker to prevent the easily guessed passwords from getting on the system in the first place according to the password cracking methods at that time, which includes trying the user's relevant personal information (name, initials, account name, etc.), trying the words from various dictionaries, and the various permutations or capitalization permutations of the dictionary words, trying the foreign language words on foreign users, and trying word pairs. Bishop and Klein [48] discuss a proactive tool for password checking called "passwd+". Bishop and Klein [8] design another proactive password checker "pwcheck" offering facilities to detect whether the passwords are easily guessed or not. The proposed password checker embraces some characteristics including the rejecting any password in a set of common passwords (e.g. the dictionary words, passwords based on users' name or account name and passwords that are shorter than a specific length), allowing per-user and per-site discrimination in its tests, having a pattern matching facility that can be stored in tests, being easy to set up, etc. Bergadano et al. [49] introduce high dictionary compression for proactive password checking. Ur et al. [50] make a discussion on the effect of strength meters that have been deployed by many web sites to provide visual feedback on password strength, and find that the stringent meters lead users to include more digits, symbols and uppercase letters to strengthen the passwords.

3) *Password Encryption*

The password encryption protections include the hash functions and the use of salts. In the computer security and cryptography, hash functions refer to the algorithms that take a variable-size input and return a fixed-size string output as the hash value. This approach ensures that any changes on the input data will result in a different hash value. There are several common characteristics of hash function including the easy computation (easy to compute the hash value for any given message), pre-image resistance (computationally infeasible to generate a message that has a given hash), second pre-image resistance (given an input A, it is difficult to find another different input B such that they have the same hash value), and collision resistance (computationally infeasible to find two different messages with the same hash), etc. There are some commonly used hash functions such as MD2, MD5⁶ (produces a 128-bit hash value) and SHA (Secure Hash Algorithm specified in the Secure Hash Standard, which is developed by NIST and published as a federal information processing standard-FIPS PUB 180⁷). The SHA (0-3) algorithms are designed for the characteristics of fast computation and efficient implementation in hardware but these characteristics also make some disadvantages such as the ineffectiveness when preventing password cracking, such as the rainbow table attacks. Except for the encryption of the passwords, the hash function is also used mainly in the digital signatures.

⁵ <http://www.cs.jhu.edu/~yairamir/cs418/os9/tsld021.htm>

⁶ <http://tools.ietf.org/html/rfc1321>

⁷ <http://www.itl.nist.gov/fipspubs/fip180-1.htm>

A salt in cryptography and computer security specifies a random data (like the nonce) which is employed as the additional input to a one-way function that hashes a password. A new salt is generated randomly by the system for each new password. In general, a salt and a password are put together and encrypted with a hash function, and then the output hash value is stored in a file. The using of salt could efficiently slow down the pre-computed rainbow table attacks because the hackers have to hash each potential password traversing all the salts. The salts are widely used in different computer systems from the UNIX system credentials to internet security. For instance, Manber [51] designs two salts (one public and one secret) to protect the passwords. The public salt is the same function with the salt at that time while the secret salt is generated randomly when the password is entered at the first time and will be discarded by the designed system after use. The users do not need to know anything about the secret salt and the secret salt is not kept anywhere. Their experiments are tested on the password schemes based on one-way functions. The performances show that using the designed two salts without changing any other part of the encryption mechanism can make the password cracking more difficult for 100 to 1000 times.

In 1970s, the DES algorithm is used to encrypt passwords in the UNIX [52] with the later implications of DES encryption algorithm developed in late 1980s [53] [54]. After that, the Unix systems have replaced traditional DES-based password hashing function “crypt()” with stronger methods such as “bcrypt” and “scrypt” [55]. These methods are also employed by other systems. For instance, the Cisco IOS uses MD5-crypt with 24-bit salt to encrypt password⁸. Large salt values are usually employed in these methods to reduce the efficiency of offline attacking due to the drastically increased cracking time. The MD5 and SHA-1 hash functions have been broken in recent years⁹. To achieve a long-term application of the hash functions, SHA-3 is designed and adopted as the NIST FIPS hash function standard in 2012¹⁰.

4) Access Control

The general thought is that if the hackers cannot get the password (or encrypted password) files, then the password cracking efficiency will be highly reduced because that the hackers cannot perform the offline guessing. According to this analysis, the password file access control is very important and efficient for the restraint of the password cracking and this method is used in some systems. For instance, the modern UNIX operating systems store the hashed password file in the route that is accessible only to programs running with enhanced privileges [56]. Password file access control method also embraces some vulnerabilities, such as the weakness in the operating systems that allow access to the password file, accidental permission of making the password file readable, sniffing password transmit in network and weak challenge or response schemes in network protocols, etc. Steiner et al. [57]

⁸ <http://c3rb3r.openwall.net/mdcrack/download/FAQ-18.txt>

⁹ <http://www.win.tue.nl/hashclash/rogue-ca/>

¹⁰ <http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>

introduce a work to secure password-based cipher suite for transport layer security. Zhao and Yue [58] give an analysis of the security vulnerabilities in the browser-based password managers, and propose a cloud-based storage-free design to achieve a high level of security with the desired confidentiality, integrity, and availability properties.

VI. CONCLUSIONS

The interaction of authentication, privacy and integrity underlies the crucial aspects in the trust model that should be applied to be secured, of which the authentication for both users and data packets has been the well-known challenge [59]. Password remains the most widely used method to ensure the authentications. However, there is some vulnerability of the passwords, such as the offline attack, specific account attack, popular password attack, user analysis, workstation hijacking, user mistake exploitation, and electronic monitoring, etc. The hackers usually utilize these vulnerabilities of the passwords to perform their attacking. This work firstly makes a discussion of the widely used password cracking methods and classifies them into several categories including the traditional methods (stealing, defrauding, user analysis, algorithm analysis and fully guessing) and the combination with import technologies from other literatures (Markov model and Probabilistic Context-Free Grammar). Then the countermeasures for password cracking are presented in two stages including the password design stage (e.g. user education, dynamic password, use of tokens and computer generated password) and the protections after the generation of passwords (e.g. reactive password checking, proactive password checker, password encryption and password file access control). There are also some other countermeasures for password attacks such as intrusion detection measures, rapid reissuance of compromised passwords, account lockout mechanisms, automatic workstation logout and policies against similar passwords on the network devices, etc.

ACKNOWLEDGMENT

The authors are grateful to the Science and Technology Development Fund of Macau and the Research Committee of the University of Macau for the funding support for our research, under the reference No. 057/2009/A2, 104/2012/A3, MYRG076(Y1-L2)-FST13-WF and MYRG070(Y1-L2)-FST12-CS.

VII. APPENDIX

A. Appendix-A: Activity

To select a new, standard password hashing algorithm, a competition track is announced in 2013:

<https://password-hashing.net/call.html>

B. Appendix-B: Some Available Softwares

1) Cain and Abel password recovery tool:

This is a tool for Microsoft Windows, which can recover many kinds of passwords with the employing of network packet sniffing, dictionary attacks, brute-force attacks,

cryptanalysis attacks and rainbow tables. [<http://www.oxid.it/cain.html>]

2) *John the Ripper password cracker:*

John the Ripper is free and Open Source software that is distributed primarily in source code. It is initially developed for Unix OS but now can run on different platforms, e.g. DOS, BeOS, Win32, etc. It combines different password crackers (including dictionary attack and brute-force modes) together with additional modules that can further extend its ability. [<http://www.openwall.com/john/>]

3) *Dave Grohl password cracker:*

It is a brute-force password cracker supporting dictionary attacks and distributed mode, which is suitable for all of the standard Mac OS X users. [<http://www.davegrohl.org/>]

4) *ElcomSoft Wireless Security Auditor:*

ElcomSoft Wireless Security Auditor under the company of ElcomSoft is a program that tries to guess the password associated with a wireless network using brute-force cracking methods and WPA/WPA2 Hash codes. [<http://www.elcomsoft.com/>]

REFERENCES

- [1] Menezes A. J., Oorschot P. C. V., Vanstone S. A., Rivest R. L. Handbook of Applied Cryptography, CRC Press. 1997.
- [2] Stallings W., Cryptography and Network Security, Prentice Hall; 4th Edition, 2005.
- [3] Pfleeger C. P., Pfleeger S. L. Security in Computing, 4th Edition, Prentice Hall, 2006.
- [4] Stallings W., Brown L. Computer Security: Principles and Practice, Prentice Hall, 2nd Edition, 2011.
- [5] Wood H. M. The use of passwords for controlled access to computer resources, NBS Special Publication 500-9, U.S. Dept. of Commerce/NBS, May 1977.
- [6] Dasgupta D., Saha S. A biologically inspired password authentication system. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIRW '09), 2009. Frederick Sheldon, Greg Peterson, Axel Krings, Robert Abercrombie, and Ali Mili (Eds.). ACM, New York, NY, USA, Article 41, 4 pages.
- [7] Seeley D. Password cracking: a game of wits. Found in: Communications of the ACM, Vol 32, No. 6 (June 1989), 700-703.
- [8] Bishop M., Klein D.V. Improving system security via proactive password checking. Computers & Security, Volume 14, Issue 3, Pages 233-249. 1995.
- [9] Landwehr C. E. Computer security. International Journal of Information Security. Volume 1, Issue 1, pp 3-13. August 2001. Springer.
- [10] Morris R., Thompson K. Password Security: A Case History. Commun. ACM, vol. 22, no. 11, pp. 594-597, 1979.
- [11] Jobusch D.L., Oldehoeft A.E. A survey of password mechanisms: Weaknesses and potential improvements. Part 1 . Computers & Security, Volume 8, Issue 7, Pages 587-604. November 1989a.
- [12] Jobusch D.L., Oldehoeft A.E. A survey of password mechanisms: Weaknesses and potential improvements. Part 2 . Computers & Security, Volume 8, Issue 8, Pages 675-689. December 1989b.
- [13] Spafford E. H. OPUS: Preventing weak password choices. Computers & Security, Volume 11, Issue 3, May 1992, Pages 273-278. 1992a.
- [14] Spafford E. Observations on Reusable Password Choices. in Proceedings of the 3rd USENIX Security Workshop, 299-312, 1992b.
- [15] Cazier J. A. and Medlin D. B. Password security: An empirical investigation into e-commerce passwords and their crack times. Information Security Journal: A Global Perspective, vol. 15, no. 6, pp. 45-55, 2006.
- [16] Marechal S. Advances in password cracking. Journal in Computer Virology, vol. 4, no. 1, pp. 73-81, February 2008.
- [17] Snyder R. Ethical hacking and password cracking: a pattern for individualized security exercises. In Proceedings of the 3rd annual conference on Information security curriculum development (InfoSecCD'06). ACM, New York, NY, USA, pp. 13-18. 2006.
- [18] Furnell S. An assessment of website password practices. Computers & Security, Volume 26, Issues 7-8, December 2007, Pages 445-451.
- [19] Plaga R. Biometric keys: suitable use cases and achievable information content. International Journal of Information Security. Volume 8, Issue 6, pp 447-454. 2009. Springer.
- [20] Winder D. Top ten password cracking methods: <http://www.pcpro.co.uk/features/371158/top-ten-password-cracking-techniques> (retrieved, April 1st, 2013)
- [21] Bonneau J., The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. Found in: Security and Privacy, IEEE Symposium on. Issue Date:May 2012. pp. 538-552.
- [22] Kelley P. G., Komanduri S., Mazurek M. L., Shay R., Vidas T., Bauer L., Christin N., Cranor L. F., Lopez J. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. Found in: 2012 IEEE Symposium on Security and Privacy. Issue Date:May 2012. pp. 523-537.
- [23] Zhang W., Zhang M., Liu Y., Wang R. A New Time-Memory-Resource Trade-Off Method for Password Recovery. Found in: Communications and Intelligence Information Security, International Conference on. Issue Date:October 2010a. pp. 75-79.
- [24] Klein D.V. Defending against the Wily Surfer - Web-based Attacks and Defenses. Proceedings of the 1st USENIX Workshop on Detection Symposium and Network Monitoring, Santa Clara CA, April 1999.
- [25] Houshmand S., Aggarwal S. Building better passwords using probabilistic techniques. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). ACM, New York, NY, USA, 109-118. 2012.
- [26] Cole E. Network Security Bible. Second edition, Ronald Krutz and James W. Conley Edited. Wiley Publishing, Inc. 2009.
- [27] Dandass Y.S. Using FPGAs to Parallelize Dictionary Attacks for Password Cracking. Found in: Hawaii International Conference on System Sciences. Issue Date:January 2008. pp. 486-493.
- [28] Berger Y., Wool A., Yeredor A. Dictionary attacks using keyboard acoustic emanations. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06), 2006. ACM, New York, NY, USA, 245-254.
- [29] Kedem G., Ishihara Y. Brute force attack on UNIX passwords with SIMD computer. In Proceedings of the 8th conference on USENIX Security Symposium - Volume 8 (SSYM'99), Vol. 8. USENIX Association, Berkeley, CA, USA, 8-8. 1999.
- [30] Theoharoulis K., Papaefstathiou I., Manifavas C. Implementing Rainbow Tables in High-End FPGAs for Super-Fast Password Cracking. Found in: International Conference on Field Programmable Logic and Applications. Issue Date:September 2010. pp. 145-150.
- [31] Oechslin P. Making a faster cryptanalytic time-memory trade-off. In Proc. CRYPTO '03, volume 2729 of LNCS, pages 617-630. Springer, 2003.
- [32] Mentens N., Batina L., Preneel B., Verbauwhede I. Time-Memory Trade-Off Attack on FPGA Platforms: UNIX Password Cracking. Proceedings of the International Workshop on Reconfigurable Computing: Architectures and Applications. Lecture Notes in Computer Science, Volume 3985, pages 323-334, Springer, 2006.
- [33] Narayanan A., Shmatikov V. Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff, CCS'05, November 7-11, Alexandria, Virginia. 2005.
- [34] Dell'Amico M., Michiardi P., and Roudier Y. Password strength: an empirical analysis. In Proceedings of the 29th conference on

- Information communications (INFOCOM'10). IEEE Press, Piscataway, NJ, USA, 983-991. 2010.
- [35] Openwall. John the Ripper password cracker, Available <http://www.openwall.com/john/> (Retrieved April 3rd, 2013).
- [36] Schneier B. Schneier on security: Choosing secure passwords. January 2007. Available: http://www.schneier.com/blog/archives/2007/01/choosing_secure.html (visited April 6th, 2013).
- [37] Weir M., Aggarwal S., de Medeiros B., Glodek B. Password cracking using probabilistic context-free grammars. in IEEE Symposium on Security and Privacy. IEEE, pp. 391–405. May 2009.
- [38] Rao A., Jha B., Kini G. Effect of grammar on security of long passwords. In Proceedings of the third ACM conference on Data and application security and privacy (CODASPY '13). ACM, New York, NY, USA, 317-324. 2013.
- [39] Shay R., Komanduri S., Kelley P. G., Leon P. G., Mazurek M. L., Bauer L., Christin N., Cranor L. F. Encountering stronger password requirements: user attitudes and behaviors. In Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10). ACM, New York, NY, USA, , Article 2 , 20 pages. 2010.
- [40] Komanduri S., Shay R., Kelley P. G., Mazurek M. L., Bauer L., Christin N., Cranor L.F., Egelman S. Of passwords and people: measuring the effect of password-composition policies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11). ACM, New York, NY, USA, 2595-2604. 2011.
- [41] Zhang Y., Monroe F., Reiter M. K. The security of modern password expiration: an algorithmic framework and empirical analysis. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). ACM, New York, NY, USA, 176-186. 2010.
- [42] Györfy J. C., Andrew F. Tappenden, James Miller. Token-based graphical password authentication. *International Journal of Information Security*. Volume 10, Issue 6 , pp 321-336. 2011. Springer.
- [43] Molloy I., Li N. Attack on the GridCode one-time password. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11). ACM, New York, NY, USA, 306-315. 2011.
- [44] Chiasson S., Alain Forget, Robert Biddle, P. C. van Oorschot. User interface design affects security: patterns in click-based graphical passwords. *International Journal of Information Security*. Volume 8, Issue 6, pp 387-398. 2009. Springer.
- [45] Weir M., Aggarwal S., Collins M., Stern H. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). ACM, New York, NY, USA, 162-175. 2010.
- [46] Yan J. J. A note on proactive password checking. In Proceedings of the 2001 workshop on New security paradigms (NSPW '01). ACM, New York, NY, USA, 127-135. 2001.
- [47] Klein D. V. Foiling the Cracker: A Survey of, and Improvements to, Password Security. Proceedings of the Unix Security Workshop II / 4th USENIX Security Workshop. Page(s): 1 – 17. Publisher: USENIX. 1990.
- [48] Bishop M., Klein D.V. Achieving Password Security through Proactive Checking. *Computers and Security* 14(3), 1992.
- [49] Bergadano F., Crispo B., and Ruffo G. High dictionary compression for proactive password checking. *ACM Trans. Inf. Syst. Secur.* 1, 1 (November 1998), 3-25.
- [50] Ur B., Kelley P.G., Komanduri S., Lee J., Maass M., Mazurek M. L., Passaro T., Shay R., Vidas T., Bauer L., Christin N., Cranor L. F. How does your password measure up? the effect of strength meters on password creation. In Proceedings of the 21st USENIX conference on Security symposium (Security'12). USENIX Association, Berkeley, CA, USA, 5-5. 2012.
- [51] Manber U. A simple scheme to make passwords based on one-way functions much harder to crack. *Computers & Security Journal*, Volume 15, Issue 2, Pages 171-176. Elsevier. 1996.
- [52] Federal Register. Federal Information Processing Data Encryption Standard, Federal Register (40FR12134), 17 Mar. 1975.
- [53] Feldmeier D.C., Karn P.R. UNIX password security-ten years later. *CRYPTO Proceedings*, 1989.
- [54] Bishop M. An application of a fast data encryption standard implementation. *Computing Systems*, 1(3), 221-254. 1988.
- [55] Provos N., Mazières D. A Future-Adaptable Password Scheme. Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference. Monterey, California, USA, June 6-11, 1999. The USENIX Association. 1999.
- [56] Singer A. No Plaintext Passwords. ;login: the magazine of USENIX & SAGE, Special Focus Issue: Security, Guest Editor Rik Farrow, volume 26, number 7: 83–91. The Advanced Computing Systems Association & The System Administrators Guild. 2001.
- [57] Steiner M., Buhler P., Eirich T., Waidner M. Secure password-based cipher suite for TLS. *ACM Trans. Inf. Syst. Secur.* 4, 2 (May 2001), 134-157.
- [58] Zhao R., Yue C. All your browser-saved passwords could belong to us: a security analysis and a cloud-based new design. In Proceedings of the third ACM conference on Data and application security and privacy (CODASPY '13). ACM, New York, NY, USA, 333-340. 2013.
- [59] Meyer H. Cracking the complex world of security. *Computers & Security*, Volume 15, Issue 3, Page 224. 1996