Applied Mathematical Sciences, Vol. 8, 2014, no. 117, 5823 - 5830
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2014.47579

An Analysis of Markov Password Against Brute Force Attack for Effective Web Applications

S. Vaithyasubramanian

Sathyabama University, Chennai, Tamilnadu, India

A. Christy

Sathyabama University, Chennai, Tamilnadu, India

D. Saravanan

Sathyabama University, Chennai, Tamilnadu, India

Abstract

Computer is omnipresent. With massive growth in the field of computers, advancement in digital technology, development in software's gives improvement to computer field on one side. Hacking the systems and cracking the login Passwords makes the field in endure on the other hand. Authentication to access an application in networks is mostly based on alphanumeric Password. A novel method of Alphanumeric Password for improving the security is "The Markov Password". Markov Passwords are created using the model of the Markov chain. This technique can be used as authentication for web applications. Password Crackers use different techniques with available large number of tools to crack down Password easily. Common attacks on Password s are Brute force attack, Dictionary attack and Hybrid attack. In this paper, a report on a study of brute force attack on Markov Passwords has been done. Analysis on Markov Password against Brute force attack is carried out using two open source tools. For analysis 40 random Password generated by Markov Chain are considered. The results are incorporated by means of graph: Password vs. Seconds to crack that Password. Average time, Maximum and Minimum time to crack Markov Password are also

tabulated. Comparative analysis has been carried out and based on that suggestions are given to create strong Markov Password for Secured System.

Keywords: Password Authentication; Information Security; Alphanumeric Password; Markov Password; Brute force Attack

1 Introduction

In cryptanalysis, there are a few regular attacks that can be used to crack the system, algorithm, or the cipher text itself. Brute-force Attack is the most "infallible" attack and it is an application of Brute force search. This is almost a foolproof attack to anything. The theory is, if crackers or attackers apply enough computing power, by all possible combinations they can try every Password in the key space to crack the file. The Brute force attack is also called as an exhaustive key search attack [2]. It is a trial and error technique. Rather than employing a scholarly approach, through extensive attempt, by using programs, tools attackers crack the encrypted data such as Passwords or Data Encryption Standard keys. In a brute force attack, programmed software is used to cause an immense number of successive guesses as to the importance of the preferred data [3]. Criminals may use these techniques to take advantage to crack encrypted data. To analyze an organization's network security, analysts implement these techniques to determine the vulnerabilities in their system. Huge numbers of successive guesses are generated using Programmed software so as to utilize the significance of the preferred data.

Brute force Attack is a method of breaking a cipher, cracking a Password by trying every possible key. The Brute force attack is a method of defeating a cryptographic scheme by systematically trying a large number of possibilities. The Brute force attack is a large amount of time-consuming method due to the number of likely arrangement of letters, numbers and special characters [1, 4]. To come across the right Password additional complex brute force attacks entail trying all key combinations in an attempt. The attacker may have a list of words or regularly used Passwords and tries all sequences of words from beginning to end to achieve the access to a login account or system. Possibility of brute force attack depends on (i) the length of the Password (ii) the complexity of the Password (iii) the strength of the Password (iv) the amount of computational power being utilized to carry out the attack (v) how good enough the attacker knows the target. Even though a brute-force attack might be capable to achieve illegal admittance to an account in the long run, these attacks can take quite a lot of hours, days, months, and even years to run. With an increase in the length of the Password the resources vital for brute force attack scale raises exponentially this would not be linear [4, 7].

To conquer from this brute force attack user can create their Passwords with

the following criteria. (i) Length of the Password is at least 10 characters long (ii) Must not be a dictionary word (iii) Repetition of Characters is to be avoided (iv) Password doesn't enclose frequent proper noun (v) Password with a mixture of all upper case, Lower case, Special characters and numbers [5, 6].

In this paper the focus is specifically on brute force attack on Markov Password. The estimated time to crack Markov Password is calculated with the help of available open source tool online Password-checker[18] and blog.kaspersky [17] for a sample of 40 chosen at random of varying length.

2 Markov Password – Alphanumeric Password

For web applications and to access resources available through networks, user ID gives identification about the user while the Password created by users alone gives whether he or she is the authenticated user. Human created Passwords generally falls in the small area [16]. The recent reveal in password shows users tendency in creating their login Passwords [19, 22]. Service provider suggests the user to create strong Passwords, but Human consideration ability tends them to create their passwords as simple as that they can recall easily [11]. The prying eyes that are enthusiastic in knowing what exist in others mailing accounts, what sort of information stored in, tends hackers to crack Password by various Password attacks [2, 21]. Private data's will get leak once password get cracked. This leads to information and data loss. To defeat this issue, moreover, to create a strong Password an innovative way has given by grouping the character sets and Password creation by directions called "Markov Password" [8].

Markov Password is a novel way to create alphanumeric Password. It is alternative ways to create Password instead of creating easily crackable common and obvious Password. Markov Passwords are created by using the theory of Markov Chain. The viable keyboard input characters are categorized in to four sets {U, L, N, S}, where they refers 26 - Upper case, 26 - lower case, 10 - Numerical and 32 - Special characters respectively. Password creation procedure is based on Markov chain i.e.) the choice of choosing the $(n + 2)^{Th}$ position character depends on $(n + 1)^{Th}$ and n^{Th} position character chosen in advance. The character takes up $(n + 2)^{Th}$ position should not from either of characters on $(n + 1)^{Th}$ and n^{Th} position character choose earlier. User decides the length of the Password, and then user can choose characters from the state spaces to frame their Password according to the rule. Bayesian Analysis on Markov Password shows the probability for character selection is 5.205% while it is 1.064% for Common Password [9].

The human mentality usually has a propensity to drift towards ease zones on Password setting [10]. Human created Passwords are mostly simple, dictionary words, family name, pet name, corner of keyboard, obvious Password or easily guessable words [12 - 15]. Pitfall in creating the Password tends the cracker to

crack them easily with available resources. Vulnerability in setting Password makes enthusiastic hackers to crack the Password by various techniques like Guessing attack, Dictionary attack, Phishing and brute force attack [20, 21]. Various key combinations make Markov Password free from dictionary words and also not to guess easily. Brute force attack on Markov Password is carried in the following section.

3 Brute-force attack cracking time estimate and Key Search Space

Brute Force Attack method explores all possible keys to attain the correct key combinations [7]. In this paper we focus particularly on brute force attack on Markov Password. Estimation of Brute-force attack cracking time for Passwords of length eight is as follows.

The key space of the entire feasible range of Passwords to search is determined using the following procedure. Key Space = L ^ (m) + L ^ (m+1) + L ^ (m+2) +..... + L ^ (M) Where, L = the length of the character set; m = minimum length of the key; M = maximum length of the key. The search space for Password by brute force attack is as follows: For Password of one to eight typescripts. Number of key search = (94 ^ 1) + (94 ^ 2) + (94 ^ 3) + (94 ^ 4) + (94 ^ 5) + (94 ^ 6) + (94 ^ 7) + (94 ^ 8). For Passwords of at least six typescripts long. Number of key search = (94 ^ 6) + (94 ^ 7) + (94 ^ 8) = 689869781056 + 64847759419264 + 6095689385410816 = 6161227014611136.

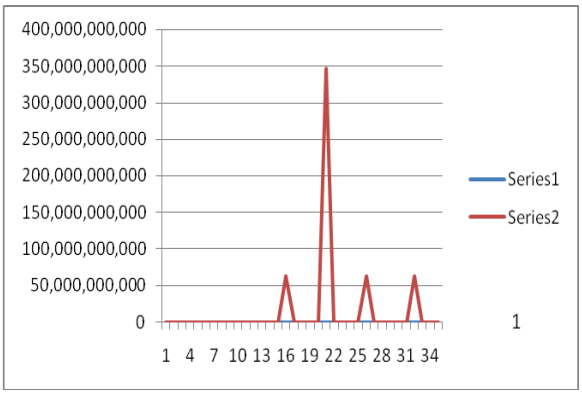
40 Markov Passwords have been chosen analyzed and compared with common Password. Estimated time to crack Markov Password and common Password by the brute force attack is presented graphically. Online Password-checker [18] and blog.kaspersky [17] open Password checker tools are used for analysis. The graphs are plotted in favor of Password vs. Estimation time to crack those Passwords using Brute force attack. The following table and figures shows attack time in seconds for Markov Password.

For Markov Password						
In Seconds	Standard Desktop PC	Fast Desktop PC	GPU	Fast GPU	Parallel GPUs	Medium size botnet
Average	15340251812	2833105838	129943235	65024793	6229857	1359
Maximum	346896000000	94608000000	2775168000	1387584000	126144000	28800
Minimum	55	14	6	3	0	0
For Common Password						
Average	1070	270	102	55	5	0
Maximum	28800	7200	2820	1440	120	0
Minimum	0	0	0	0	0	0

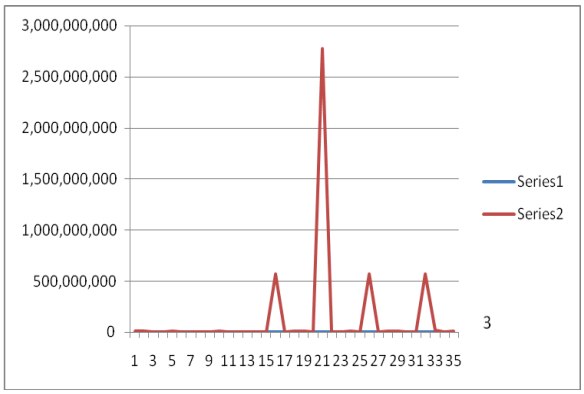
Table: 1 Attack estimation time estimated by Password -checker. Online-domain-tools

For Markov Password				
In Seconds	ZX Spectrum The popular home computer from 80s	*Mac Book Pro (2012) Popular laptop with powerful Intel Core i7 CPU	Conficker botnet One of the most prolific botnet	Tianhe-2 Supercomputer The world's fastest supercomputer
Average	9149397097783	3673598742072	30357054915	198704590
Maximum	31536000000000	31536000000000	958694400000	6307200000
Minimum	604800	420	1	1
For Common Password				
Average	3	1	1	1
Maximum	4	1	1	1
Minimum	2	1	1	1

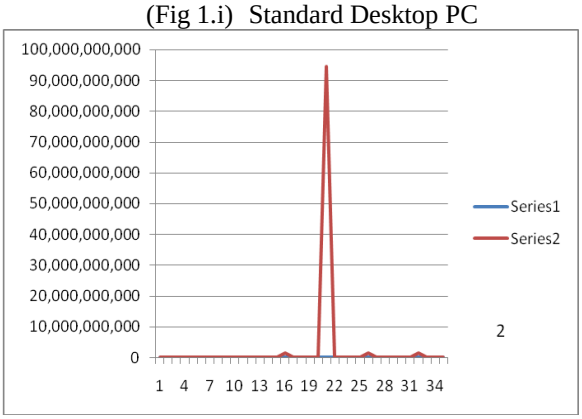
Table: 2 Attack estimation time estimated by blog.kaspersky.com/Password -check



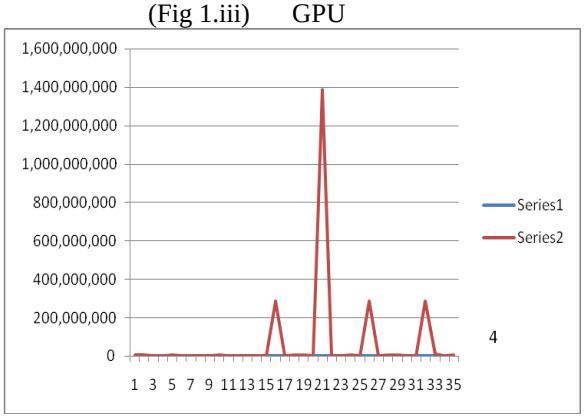
(Fig 1.i) Standard Desktop PC



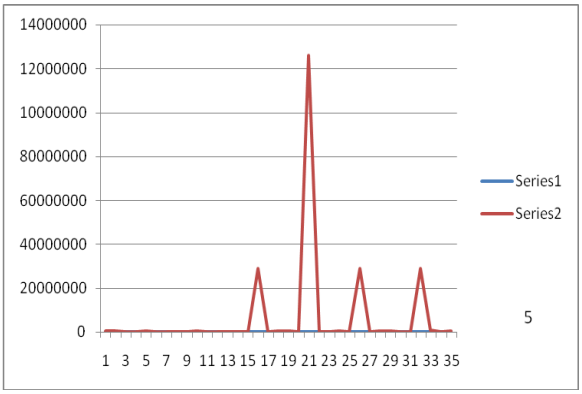
(Fig 1.iii) GPU



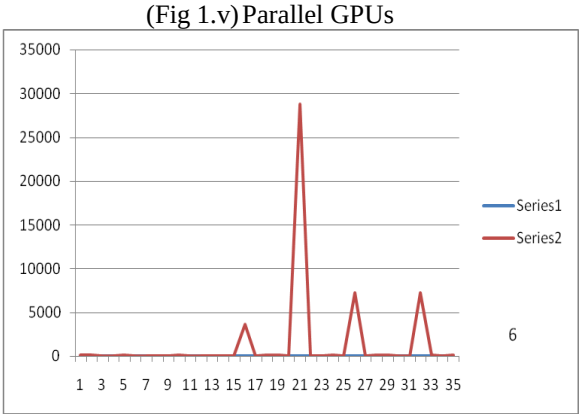
(Fig 1.ii)Fast Desktop PC



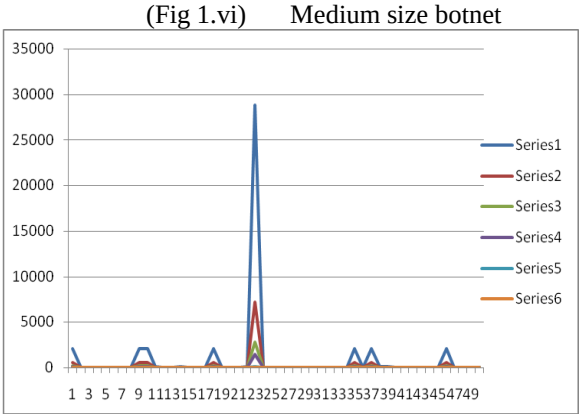
(Fig 1.iv) Fast GPU



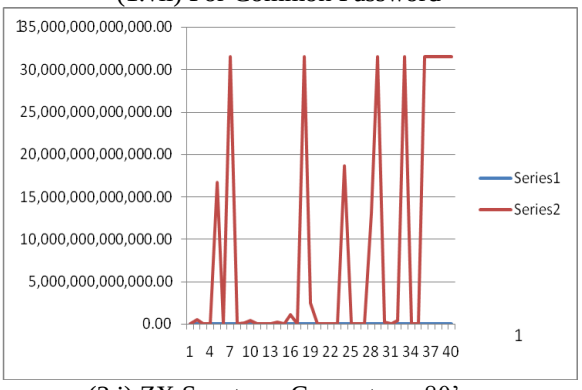
(Fig 1.v) Parallel GPUs



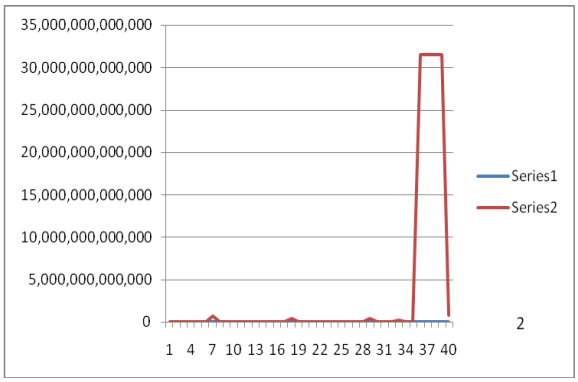
(Fig 1.vi) Medium size botnet



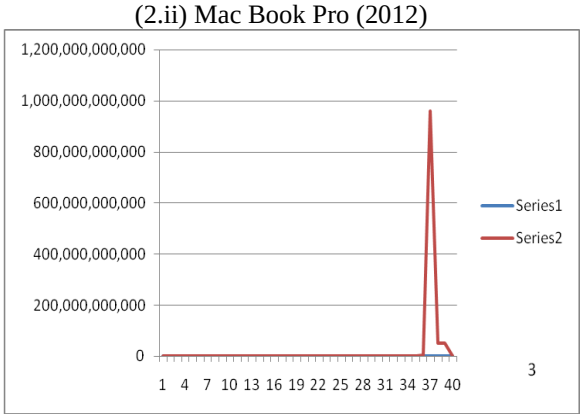
(1.vii) For Common Password



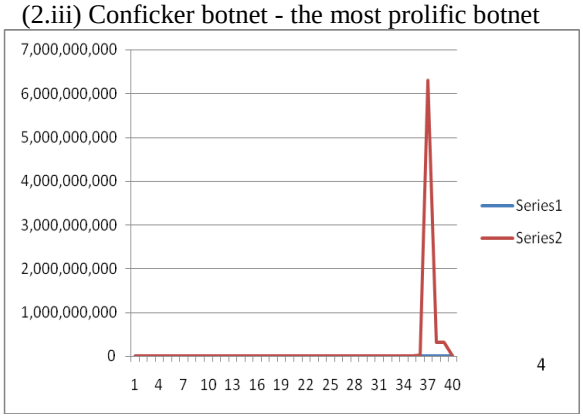
(2.i) ZX Spectrum Computer – 80's



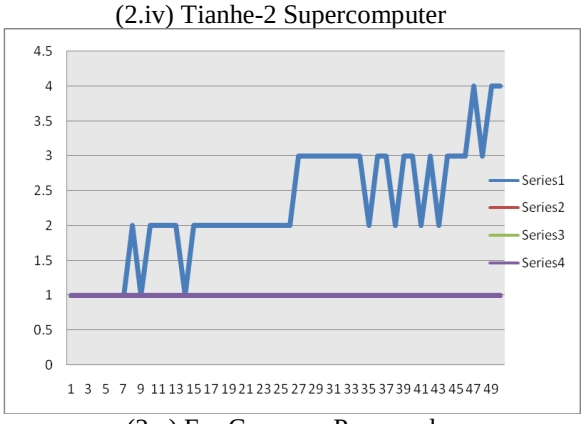
(2.ii) Mac Book Pro (2012)



(2.iii) Conficker botnet - the most prolific botnet



(2.iv) Tianhe-2 Supercomputer



(2.v) For Common Password

Conclusion

Believability of brute force attack depends on the key length of the Password. And the amount of computational supremacy available on the hand of the cracker. The brute force attack is impractical aligned with the Passwords with fickle dimension input. From the tables 2 and 3 showing the average, upper limit and minimum estimation time to crack Password it is clear that to a larger extent for Markov Password it will require more time to crack than the common Password. The reason may be the foundation of categorization of character space into four groups and Password creation by various key combinations. This paves a new path for effective data and network security. Good resistance towards brute force attack shows Markov Password can be effectively used as Password authentication for network applications. At the same time supporting research and user study is necessary to carry out high level of growth and functioning.

References

[1]. Jim Owens and Jeanna Matthews "A Study of Passwords and Methods Used in Brute force SSH attack" In USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008.

[2]. Mudassar Raza, Muhammad Iqbal et. al "A survey of Password Attacks and Comparative analysis on methods for secure Authentication" World Applied Science Journal 19(4) : 439 – 444, 2012.

[3]. Neeraj Kumar "Investigations in Brute force attack on Cellular Security Based on Des and Aes" International journal of Computational Engineering & Management, Vol 14, 50 – 52, October 2011.

[4]. Richard Clayton "Brute force attack on cryptographic keys"- file:////H:/brute force attack / brute.html, Oct 2001.

[5]. Carlisle Adams, Guy-Vincent Jourdan, Jean-Pierre Levac and Francois Prevost "Lightweight Protection against brute force login attacks on web applications"PST, 181 – 188, IEEE – 2010.

[6]. http://www.infosecpro.com/applicationsecurity/a11.htm.

[7]. http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/

[8]. Vaithyasubramanaian.S and A. Christy "A Scheme to Create Secured Random Password using Markov Chain" – SPRINGER International Conference on Artificial Intelligence and Evolutionary Algorithm in Engineering Systems – ICAEES 2014.

[9]. Vaithyasubramanaian.S and A. Christy "A Study on Markov Chain Password using Bayesian Inference" Ciit Journal Artificial intelligent Systems and Machine Learning, Vol 6, No 3, 100-102, 2014.

[10]. Jeff Yan, Alan Blackwell, Ross Anderson, Alasdair Grant "Password Memorability and Security: Empirical Results" IEEE security & privacy Vol: 2, Issue: 5, 2004, Page No. 25 – 31.

[11]. Edward F. Gehringer "Choosing Passwords: Security and Human factors" IEEE 2002 international symposium on Technology and Society, (ISTAS'02), ISBN 0-7803-7284-0, Page No. 369 – 373.

[12]. Bander AlFayyadh, Per Thorsheim, Audun Josang and Henning Klevjer "Improving Usability of Password Management with Standardized Password Policies" The Seventh Conference on Network and Information Systems Security - SAR-SSI 2012 Cabourg, May 2012, ISBN 978-2-9542630-0-7.
[13]. Sarah Granger, "The Simplest Security: A Guide To Better Password Practices" - http://www.symantec.com/connect/articles, July 2011.
[14]. Dinei Florencio, Cormac Herley, Baris Coskun "Do strong Web Passwords Accomplish Anything?" Proceeding HOTSEC'07 Proceedings of the 2nd USENIX workshop on Hot topics in security, ACM Digital Library, 2007.
[15]. Dinei Florencio, Cormac Herley " A Large-Scale Study of Web Password Habits" Proceedings of the 16th international conference on the World Wide Web, ACM Digital Library, 2007, Page No. 657-666.
[16]. Jason Hong "Passwords Getting Painful, Computing Still Blissful" Communications of the ACM I MARCH 2013 I Vol.56 I No. 3.
[17]. http://blog.kaspersky.com/Password -check/
[18]. http://Password -checker. online-domain-tools.com/
[19]. http://www.zdnet.com/the-top-10-passwords-from-the-yahoo-hack-is-yours-one-of-them-7000000815/
[20]. http://resources.infosecinstitute.com/dictionary-attack-using-burp-suite.
[21]. www.ghacks.net/2013/10/26/4-simple-password-creation-rules-x-common-sense-tips/
[22]. http://news.in.msn.com/gallery/these-are-the-worst-passwords-of-2013-1#image=1.

Received: July 7, 2014