Volume-4, Issue-5, May-2015 • ISSN No 2277 - 8160

Research Paper | Engineering

Comparative Analysis and Study between Markov Password and CFG Password

S.Vaithyasu bramanian	Research Scholar, Sathyabama University, Chennai.
A. Christy	Research Supervisor, Sathyabama University, Chennai.
D.Saravanan	Faculty of Operations & IT, IBS Hyderabad.

ABSTRACT

Seeing that the computer and internet technology grows with immense expansion, these days everyone holds an email and online account. Starting from reading newspaper online, communicating with others through email, connecting stay with friends and relatives through social networks, online ticketing, online shopping and internet banking almost everyone is using their computer gadget and right to use internet. Confirmation to Logging-in to their login account is one of the procedural processes carried out with a username and password. Password proves that he/she is the authenticated user while username gives his/her identity. Essential Authentication has just obliged a username and Password. Ineffective mistake when one makes at the time of creating login account and Password cause their login account vulnerable against hacking and intrusion. In view of the fact that the Password is the gateway for accessing their account after getting prior approval from the administrator, a password should be the deterrent to various sorts of attacks. Such innovation in creating and generating alphanumeric passwords is Markov Password and CFG Password. In this paper, we furnish comparative analysis and study between Markov Password and CFG Password. Analysis shows how, where and when these two Password techniques can be utilized. This technique paves a new way for authentication process.

KEYWORDS : Data Security - Login - Authentication - Password - Markov Password - CFG Password.

Introduction

Passwords are privileged insights that stay secretive to a person who expects to utilize it to confirm oneself. A Password is a torrent of characters (letters in order, numbers and/or extraordinary characters) that is utilized by people to validate them, to demonstrate who they say they are. Passwords are not used to demonstrate ones personality alone, they are utilized as checkpoints to give access to assets. In the present days, validation has developed and gone past passwords, to demonstrate you are who you say you are. Verification has been extemporized on everyday schedule to have different approaches to confirm the clients: (i) what you know, for example, alphanumeric Password, Graphical Password, (ii) what you have, for example, Smart cards, ATM cards and so on and (iii) what you are - biometric Authentication. One or a greater amount of these validations could be consolidated to build the proficiency of confirming a person. That is, "The thing that you know?" could be joined with "What you have" to make it a solid verification process. Albeit, there are numerous approaches to join verification plans and there are numerous modern validation plans, passwords are thought to be the most utilized confirmation system even today. This is the reason, we needed to offer significance to passwords and have a different space recently to help individuals understand the significance of passwords.

Alphanumeric passwords were initially presented in the 1960s as an elucidation for security issues that got to be obvious as the first multi-client operating systems were being produced. As the name shows, an alphanumeric secret word is basically a series of letters and digits. Albeit any string can serve as a secret gateway, these passwords just offer great security the length of they are sufficiently entangled so that they can't be found or speculated. Regular rules for alphanumeric Passwords: The Password (i) ought to be not less than 8 characters in length. (ii) Ought not to be anything but difficult to identify with the user (e.g., last name, birth date). (iii) Ought not to be a word that can be found in a lexicon or open registry. (iv) Ideally, the user ought to consolidate upper and lower case letters and digits.

Basic Authentication is a design that uses an encoded username and Password for credentials. Verification is the methodology of the client, demonstrating its character to the server. Credentials are secrecy bits of data used to demonstrate the customer's personality (username, password...). At the point when client validate with a server, client demonstrates his/her identity to the server by letting it know data that just the client knows. Once the server knows who the client is, it can trust client and reveal the private information in his/her record. The client takes these two certifications, smooshes them together to frame a single esteem, and passes that along in the appeal in a HTTP header called Authorization. At the point when the server gets the solicitation, it takes a gander at the Authorization header and contrasts it with the accreditations it has put away. On the off chance that the username and secret key match one of the clients in the server's rundown, the server satisfies the customer's appeal as that client. On the off chance that there is no match, the server gives back a unique status code (401) to tell the user that confirmation fizzled and the appeal is denied. Since the best Password would be a totally random one, individuals have formulated approaches to make random passwords. In any case, the better the Password is, the harder it is to recollect. The disadvantages of alphanumeric Passwords are they are exposed to various types of attacks. The vulnerabilities in creating their password and other pitfalls such as weak Password, obvious Password, easily guessable Password, dictionary word, Key board corner keys as Password, same Password for all Logins, writing down their Password in piece of paper or on their diary, asking the system to remember their Password, installing unauthorized Password management system in maintaining their Password, storing the record of Password in their mail account, sharing Password with others and etc puts together the intruders to crack Password and to gain the users login account.

New techniques in creating and generating alphanumeric Password are Markov password and CFG Password. Markov Password and CFG Password are type of random Password can be created, generated by their unique methodology. In this paper, we present a comparative study and analysis between these two Password techniques. The comparison has been furnished in the form of a table. Next two section deals with Markov Password and CFG Password, in section 4 comparative analyses and study on these two techniques are presented in tabular form and followed by discussion and conclusion.

2. Markov Password

Markov Password creation or generation technique is as follows: This Password creation system is taking into account the idea of Markov chain the discrete random process of Markov Process. Markov chain is a stochastic model portraying a succession of possible occurrence in which the likelihood of every occasion depends just on the state achieved in the past occasion. A Markov chain is an arrangement of arbitrary variables {X1, X2, X3…}, Xi's from a countable set called state space of the chain, having the property that the current state depends only on the previous past state not depending on the past states. i.e) the state X3 depends only on the state X2 not on X1 or X0. The conceivable console info characters are sorted into four sets {U, L, N, S}, where they represent 26 - Uppercase, 26 - lowercase, 10 - Numerical and 32 - Special characters individually. At first the user needs to choose the length of the secret key, then the user can pick any of the characters from the four state spac-

es characterized and can proceed with the methodology. If the user chooses any one of the characters from state space L in the first place, then the user can select any one of the characters from U or S or N for the second position. If the user choice is L then for the third position the user cannot choose either from U or L. The process continues until character selection and the length chosen by the user matches equally. The decision of picking the $(n + 2)^{th}$ position character relies on upon $(n + 1)^{th}$ and n^{th} position character picked before. The character possesses $(n + 2)^{th}$ position ought not from both of the characters on $(n + 1)^{th}$ and n^{th} position character picked before.

2.1 Markov Password Illustration:

1	Way	L	U	N	S	U	L	S	N
	Password	b	O	5	$	M	i	(	3
2	Way	L	S	U	N	L	S	N	U
	Password	r	@	V	1	r	@	9	I
3	Way	N	S	L	N	U	L	N	U
	Password	5	0	r	8	S	a	1	D
4	Way	U	S	N	L	U	S	N	L
	Password	R	@	9	i	R	@	7	i

CFG Password:

Typical way of creating CFG Password would be as follows. A Context free grammar G is defined by 4-tuple G = (V, T, P, S) where V is a finite set of nonterminals, T is a finite set of terminals the set of terminals is the alphabet of the language defined by the grammar G, P the production rule and S the start symbol. The Grammar G generates strings which forms a language L (G). The strings of the Grammar G are derived by the production rule P which is a mapping from V to (V U T)*, where the * represents the Kleene star operation. Initially the user has to choose the grammar which generates strings by choosing input alphabets. Then the length of the Password. The password should be of minimum length 8. User can choose one of the Passwords from the strings generated from the grammar preferred by the user. Since this grammar generates patterns of strings users can choose different password for different logins. Users have to remember which pattern of string he/she have chosen as Password and for which logins. To make it complex user can use various combinations and options.

3.1 CFG Password illustration:

Language	Terminals	Production rule	Example
The word "NATURE" somewhere in the string.	a to z ; A to Z; 0 to 9; ~ to?	S → <LETTER*> NATURE <LETTER*>; <LETTER*> → <LETTER> <LETTER*> | λ; <LETTER> → a | ... | z | 0 | ….| 9 | ~ | …| <.	123NATUREabc `123NATURERst !@#NATURE$%^ ABCNATURE123
Strings of Well Balanced Parenthesis	a to z; 0 to 9 A to Z	S → LETTER + LETTER | LETTER - LETTER | LETTER * LETTER | LETTER / LETTER | (LETTER) | [LETTER] | {LETTER} | a | b | c | ….| z | 0 |. . .| 9.	(a+b)*(a-b) {(r-t) +(r*t)} [x*y]-[x-z]
Strings of unequal Numbers of a's and b's.	a, b	S → A | B; A → CaA | CaC; B → CbB | CbC; C → aCbC | bCaC | λ.	aaaabbbaba bababaaaab abbaabbabb

Comparative Analysis:

Comparison	Markov Password	CFG Password
Generation Type	Markov Chain.	Context Free Grammar.
Creation Method	Condition based.	Rule based.
Password Type	Random, Based on Rule.	Random, Based on Grammar.
Characters Used	Variety.	Rarely, depends on rule.
Usability	Password gateway / OTP.	OTP / Password gateway /
Strength	Good.	Depends on length / Grammar.
Guess ability	Hard to Guess.	Depends on Input alphabet, Grammar and Length.
Nature	Formation Method, The conditions on selecting the input alphabets.	The Grammar and production rule.
Memorability	Depends on the User	Easy, once if the rule is remembered.
Accuracy	Strength to Authentication technique.	Pattern of easily derivable strings for Authentication.
Complexity	Remembrance.	Need of study about the generation rule.
Uniqueness	Generation Principle. Variety of Keyboard character usag for password. Keeps away the users from creating obvious Passwords.	Pattern of password. Keeps away the users from creating obvious Passwords.
Integrity	Security, Resistance to attacks.	Remembrance – easily rememberable.
Affordability	Depends on user service provider.	Depends on user or service provider.
Usage	As a gateway for login accounts where the user needs more security. And for websites where intruders often try to crack Passwords.	As a gateway for login accounts where the intruders not having much interest in cracking the password. Incase if the users want to use for logins where it should be secured there the user has to choose of good combination of CFG password.
Example	R@v1Ra9I	[{a+b}+{c*d}]

Conclusion:

Password security is the key to the protection of data frameworks. A password plays the primary role in fortification against various network attacks and intrusions. Users should have a moral basic to pick great password to secure the data against the intruders, at the same time administrators have the responsibility to see that they do. Toward the end, service providers and system administrators should give guidance to their users on the most proficient method to create Password for their login accounts. Our Password methods can be implemented for effective security of the users' information protection. Comparative analysis on the two proposed password techniques states their strengths and limitations from which the users or service providers can be implemented these techniques as the Password Gateway. Future work around there ought not to let the human well enough alone for the mathematical statement.

REFERENCES

1. Bander AlFayyadh, Per Thorsheim, Audun Josang and Henning Klevjer "Improving Usability of Password Management with Standardized Password Policies"The 7th Conference on Network and Information Systems Security, abourg, May 2012. | 2. Sarah Granger, "The Simplest Security: A Guide To Better Password Practices" - http://www.symantec.com/connect/articles, July 2011. | 3. Jeff Yan, Alan Blackwell, et.al "Password Memorability and Security: Empirical Results" IEEE security & privacy, Vol.2, Issue: 5, 2004, pp 25–31. | 4. Edward F. Gehringer "Choosing passwords: Security and Human factors" IEEE international symposium on Technology and Society, pp369 – 373, 2002. | 5. 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, pp.657-666. | 6. http://resources.infosecinstitute.com/dictionary-attack-using-burp-suite. | 7. www.ghacks.net/2013/10/26/4-simple-password-creation-rules-x-common-sense-tips/ | 8. Jason Hong "Passwords Getting Painful, Computing Still Blissful" Communications of the ACM I March 2013 I Vol.56 I No. 3 | 9. www.oxforddictionaries.com/us/definition/american_english/Markov-chain. | 10. http://mathworld.wolfram.com/MarkovChain.html. | 11. Hop croft, John E.; Ullman, Jeffrey D. (1979), Introduction to Automata Theory, Languages, and Computation, Addison-Wesley. Chapter 4: Context-Free Grammars, pp.77–106. | 12. Gerhard Jagar and James Rogers "Formal Language Theory: Refining the Chomsky Hierarchy". | 13. S.Vaithyasubramanian, A. Christy, D. Saravanan "An Analysis of Markov Password against Brute Force Attack for Effective Web Applications" Applied Mathematical Sciences, HIKARI Ltd, Vol. 8, 2014, no. 117, pp5823 - 5830. | 14. S.Vaithyasubramanian, A. Christy "A Scheme to Create Secured Random Password Using Markov Chain" Advances in Intelligent Systems and Computing, Springer India, Vol. 325, 2015, pp809-814. | 15. S.Vaithyasubramanian, A. Christy "An Analysis on 1-Step Transition Probability Matrix and 2-Step Transition Probability Matrix of Markov Passwords" International Journal of Applied Engineering research, Vol. 9, Number 20, 2014 pp7745-7753. | 16. S.Vaithyasubramanian, A. Christy "A practice to create user friendly secured password using CFG" International Conference on Mathematics & Engineering Sciences, Chitkara University, Punjab, March 2014, pp39. | 17. S.Vaithyasubramanian, A. Christy "A study on Markov chain password using Bayesian inference" CiiT International Journal of Artificial Intelligent Systems and Machine Learning, Vol. 3, No 3 2014. | 18. S.Vaithyasubramanian, A. Christy "Authentication Using String Generated from Chomsky Hierarchy of Formal Grammars" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 8, 2015, pp6269-6273. | 19. S.Vaithyasubramanian, A. Christy, D. Saravanan "Two Factor Authentications for Secured Login in Support of Effective Information Preservation and Network Security" ARPN Journal of Engineering and Applied Sciences, Vol. 10, No. 5, March 2015, pp2053-2056. | 20. S.Vaithyasubramanian, A. Christy "An analysis of CFG Password against Brute Force attack for effective web applications" – Contemporary Engineering Sciences, ISSN 1313-6569 (print) ISSN 1314-7641 (online), Vol.8, No. 9, pp367-374, 2015. |