IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 5, Juy 2014.
www.ijiset.com
ISSN 2348 – 7968

An Implementation of a Secure System to Generate and Maintain Multi- Domain Password to Defend against Password Attacks

Miss Pallavi Dhole [1], Prof.S.J.Karale [2] and Miss. Pratibha Mishra [3]

[1] Student Mtech (CSE), G.H.R.I.E.T.W, Nagpur
[2] Asst.Professor (IT), Y.C.C.E, Nagpur
[3] Lecturer (CSE) , G.H.R.I.E.T.W, Nagpur

Abstract

Password is a secret word or string of character that is used for user authentication to prove identity or for access approval to gain access to a resource. Basically, password is used in every interaction between user and information system. Unfortunately, with such a central role in security, passwords are prone to attacks. Password attack is a method of gaining unauthorized accessed to one's computer or to a personal account. This attack reduces the convenience of authorized users. Different types of methods and protocols are used to reduce such attacks and prevent user's data to be accessed from unauthorized users. On the other hand users also generally prefer common and easy passwords which are weak and make online guessing attacks much easier. The password guessing resistant protocol overcomes these online guessing attacks mainly brute force and dictionary attacks. This is achieved by limiting the number of attempts made during login. The goal is to provide convenient and secured login to the authorized users which is by blocking the IP address from which there are more number of failed login attempts. Enabling convenient login for authorized users while preventing attacks is a difficult problem. We proposes a new "Gold Code Sequence Generator" (GCSG), derived upon revisiting prior proposals designed to restrict such attacks. While GCSG generates new password every time whenever an authorized user log's in and password is stored in hash form instead of any row form.

Key words: Gold Code Sequence Generator (GCSC), Password Guessing Resistant Protocol (PGRP), Password attacks, security.

1. Introduction

Passwords are the most common method of authenticating users, and will most likely continue to be widely used for the foreseeable future, due to their convenience and practicality for service providers and end-users. Although more secure authentication schemes have been suggested in the past, e.g., using public key cryptography, etc none of them has been in widespread use in the consumer market. It is a well known problem in computer security that human chosen passwords are inherently insecure since a large fraction of the users chooses passwords that come from a small domain. A small password domain enables adversaries to attempt to login to accounts by trying all possible passwords, until they find the correct one. This attack is known as a "dictionary attack". Successful dictionary attacks have, e.g., been recently reported against eBay user accounts, where attackers broke into accounts of sellers with good reputations in order to conduct fraudulent auctions.

When trying to improve the security of password based authentication, one wants to prevent attackers from eavesdropping on passwords in transit, and from mounting offline dictionary attacks, namely attacks that enable the attacker to check all possible passwords without requiring any feedback from the server. Eavesdropping attacks can be prevented by encrypting the communication between the user and the server. Offline dictionary attacks are prevented by limiting access to the password file and can be made even harder.

In our discussion here we assume that the security measures described above are already implemented and therefore the attacker can only mount online dictionary attacks. Namely, attacks where the only way for the attacker to verify whether a password is correct is by interacting with the login server. This might be a reasonable assumption for an Internet based scenario, where a new protocol namely "Gold Code Sequence Generator" protocol is designed against online attacks." GCSG" protocol is used to generate new passwords every time when ever an authorized user log's in and the server uses reasonable security measures to secure its password file.

ISSN 2348 – 7968

2. Objectives

Objectives are the key points of the research that is being carried out. The Proposed System should achieve the desired objectives. Following are objective of the proposed system against online attacks:-

- Gold Code Sequence Generator protocol is used to generate new password every time whenever an authorized user log's in into his/her account.
- Keeping track on login attempts of authorized user for a security purpose access.
- Daniel of access to authorized and unauthorized users, if accessing from same or different browser at same time.
- Security is also provided by hardware i.e. mobile

3. Literature Review

The use of passwords is a necessity in computer security but passwords are often easy to guess by automated programs or tools running dictionary attacks [3]. In the existing system, an automated test is implemented that humans can pass, but current computer programs can't pass. Any program that has high success over these tests can be used to guess passwords cause security risks. An example of such a test is a 'captcha' [4]. A captcha is a test used in computing which ensures that the response is generated by a person and not by a tool. Following figure is an example of Captcha.

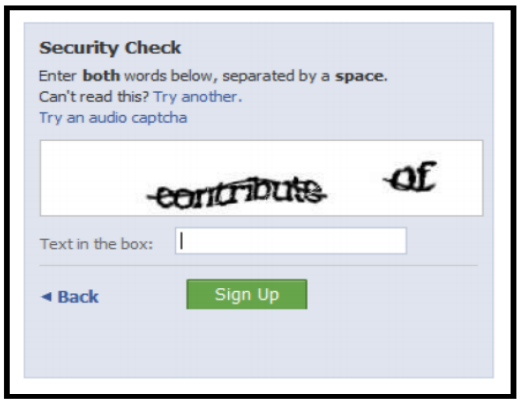

Figure 1: Example of a Captcha

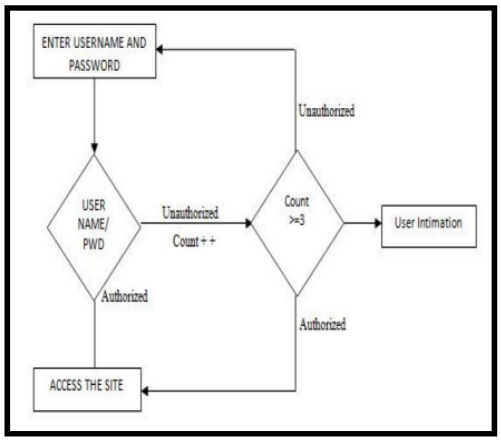

Figure2. Flow Chart of Existing System

PGRP accommodates both graphical user interfaces and character-based interfaces. PGRP enforces ATT's after a few failed login attempts are made from unknown system [2]. PGRP uses either cookies or IP addresses, or both for tracking authorized users [5]. Tracking users through their IP addresses also allows PGRP to increase the number of ATTs for password guessing attacks and meanwhile to decrease the number of ATTs for legitimate login attempts [1].

Gold Code Sequence Generator (GCSG) which is our proposed system generates a new password every time when ever an authorized user log's in into his/her personal account. Every time the new password is randomly generated. As soon as user inputs his or her username, immediate password is provided to user through a message to his/her registered mobile number and as soon as user log's out from his/her account, password gets changed. They are identified by username, IP address and by secret key saved on login server. GCSG uses IP addresses, User name, cookies and Secret key to track the authorized users. The goal is to provide convenient and secured login to the authorized users which is by blocking the IP address from which there are more number of failed login attempts. The proposed system is much more convenient than the existing system and consists of

ISSN 2348 – 7968

minimal steps for authorized user to login. Two processes are involved in this:

1) If a trusted system fails the first login attempt then it is given two more chances (totally three chances). If the user fails in the third attempt to login then the intimation will be given.

2) If an unknown system fails in the first login attempt then it will not be given any more chances and intimation.

The Gold Code Sequence Generator protocol overcomes these online guessing attacks mainly brute force and dictionary attacks [1]. This is achieved by limiting the number of attempts made during login.

4. Proposed Plan of Work

4.1) Module 1: Development of Online Login System

We are developing Online Login System module in which user will be able to login in his/her account or any other multi-domain system .This module is similar to New User Login Page, only instead of Password, User Name and Secret Key is mandatory.

4.2) Module 2: Development of Password Creation Module

In Password Creation module, we are generating random password through it. Every time when ever user log's in into his/her account, a new password will be generated by this module and will be inform to the user through message on his/her registered mobile number.

4.3) Module 3: Application of Password Guessers (like brute force) on Our System

We are developing Brute Force attackers in this module. These attackers will try to hack the password which are normally weak or can be easily guessed.

4.4) Module 4: Checking the Response of the System

As we have developed Brute Force Attackers in previous module, this module will observe response of Brute force attacks and will try to block those attacks.

5. Researched Methodology

Gold Code Sequence Generator (GCSG) which is our proposed system generates a new password every time when ever an authorized user log's in into his/her personal account Every time the new password is randomly generated. As soon as user inputs his or her username, immediate password is provided to user through message on his/her registered mobile number and as soon as user log's out from his/her account, password gets changed. They are identified by username, IP address and by secret key saved on login server. GCSG uses IP addresses, cookies, user name and secret key to track the authorized users. The Password is stored in Hash form instead of any raw form. The goal is to provide convenient and secured login to the authorized users which is by blocking the IP address from which there are more number of failed login attempts. We are keeping track on login attempts of authorized user for security access purpose. Also denial of access to authorized and unauthorized users, if accessing from same or different browser at a same time.

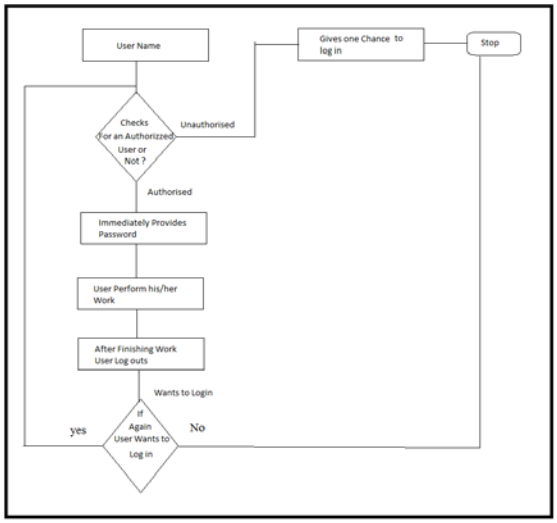

Figure 3. Flow Chart of Proposed System

ISSN 2348 – 7968

6. Expected Outcome and Future Work

The goal of proposed system is to provide convenient and secured login to the authorized users which is by blocking the IP address from where there are more number of failed login attempts. Also providing security by creating new password every time when ever authorized user log's in into his/her personal account. Using Gold Code Sequence Generator, data integrity is protected, as a secret key (IEMI number of mobile) is used while creating new user account. We are keeping track on login attempts of authorized user for security access purpose. Also denial of access to authorized and unauthorized users, if accessing from same or different browser at a same time. Security is also provided by a hardware i.e. mobile.

The further enhancement can be done by encrypting the password which is been generated and forwarded to the valid user. Even the encrypted password can be a onetime password which is been generated by the server. This method will be more authenticated which may avoid the password modification or the theft when it is been send from the browser to the valid user. In our system we can perform security and compression techniques to make the system more efficient in terms of speed and security for future purpose.

7. Conclusion

Password attacks have been increasing rapidly. To put an end to this we use GCSG. GCSG will restrict the number of attempt made by a system or a machine and allow the authorized user to have a full secured access over their account. GCSG appears suitable for organizations of both small and large number of user accounts. GCSG can restrict brute force attack and dictionary attack, so it enhances the security of user's account and it also offers more convenient login experience.

References

[1] Mansour Alsaleh, Mohammad Mannan and P.C van Ootschot, "Revisiting Defenses against Large-Scale Online Password Guessing Attacks", IEEE TRANSACTION ON DEPENDABLE AND SECURE COMPUTING, vol.9, NO.1, JAN/FEB 2012

[2] Mohd Muzaffaaruddin Arshad, Ayesha Siddiqua and Ishrath Nousheen "Resistant Protocol To Resist Large-Scale Online Password Guessing Attacks", International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Special Issue of ICACSE 2013 - Held on 7-8 January, 2013.

[3] Nitin Garg, Raghav Kukreja, Pitambar Sharma , "Revisiting Defenses against Large-Scale Online Password Guessing Attacks", International Journal of Scientific and Research Publications, vol.3 , No.4, APR 2013

[4] D. Ramsbrock, R. Berthier, and M. Cukier, "Profiling Attacker Behavior following SSH Compromises", IEEE Transation on Dependable Systems and Networks, JUN 2010

[5] J. Jayavasanthi Mabel and Mr. C. Balakrishnan"Resisting Password Based System from Online Guessing Attacks", International Journal of Emerging Technology and Advanced Engineering, vol.3 , special Issue 1, Jan 2013.