322. UGP-A PROTECTIVE MEASURE AGAINST PASSWORD ATTACKS

P.Ramkumar[1], G.Anbuselvi[2]
Department of Computer Science and Engineering
Meenakshi College of Engineering
Chennai-78, India
[1]Raamkumaar77@gmail.com, [2]g.anbuselvi.be@gmail.com

Using hard AI problem for security is emerging as an exciting new paradigm. A new security primitive based on hard AI problems, namely, a new family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is click based graphical passwords, where a sequence of clicks on an image is used to derive a password. CaRP addresses a number of security problems such as online guessing attacks, relay attacks, shoulder-surfing attacks. CaRP offers reasonable security and usability, CaRP is one step forward in the paradigm of using hard AI problems for security. In proposed system plan to improve the usability and security of the users in the internet services .Tradeoff between usability and security is the main issue in graphical passwords .Security will be improved by encrypting the user passwords using SPH (salted password hashing) and encrypted password will be stored in database. When user logins, again encrypted value will be generated using salt hashing technique and it will be compared with the hash value which is already stored in database. If both match, the password is correct. Usability will be improved by using SUS (security usability symmetry) that divides usability into four factors and login attempts will be reduced to three times. If exceeds limit, access will be blocked to user and notification will be sent to user mobile for password reset.

Index Terms—Network Security, Graphical Password, CaRP, UGP, Password Attacks, Salted Password Hashing.

Journal of Science and Innovative Engineering & Technology

ISBN 978-81-904760-6-5