Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 8, August 2013, pg.174 – 180

RESEARCH ARTICLE

OPass: Attractive Presentation of User Authentication Protocol with Resist to Password Reuse Attacks

S. Megala Devi[1], M. Geetha[2]

[1]Research Scholar, Department Of Computer Science, Vivekanandha College,
Tiruchengode, Tamil Nadu, India

[2]Assistant Professor, Department Of Computer Application, Vivekanandha College,
Tiruchengode, Tamil Nadu, India

[1] megala8800@gmail.com; [2] geethkavi19@gmail.com

Abstract— Passwords are the influential apparatus that tend to keep all data and information digitally safe. It is often notice that text password leftovers mostly popular over the other formats of passwords, due to the information that it is simple and convenient. However, text passwords are not always strong enough and are very easily stolen and changed under different vulnerabilities. Others can acquire a text password when a person creates a weak password or a password that is completely reused in many sites. In this condition if one password is stolen, it can be used for all the websites. This is called as the Domino Effect. Another risky environment is when a person enters his/her password in a computer that is not trust-worthy; the password is prone to stealing attacks such as phishing, malware and key loggers etc. In this paper, a user authentication protocol named Password is designed, that makes use of the customer's cellular phone and short message service to ensure protection against password stealing attacks. Password requires a unique phone number that will be possessed by each participating website. The registration and the recovery phases involve a telecommunication service provider. The main concept of the project is reducing the password reuse attack. We have implemented the one time password technology, and then reduce the password validity time. The performance had improved the security.

Key Terms: - Encryption; Hash Function; Network Security; One-Time Password; Password Reuse Attack; Password Stealing Attack; User Authentication

Full Text: http://www.ijcsmc.com/docs/papers/August2013/V2I8201342.pdf