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. 3, Issue. 2, February 2014, pg.815 – 826

RESEARCH ARTICLE

Implementation of Password Guessing Resistant Protocol (PGRP) to Prevent Online Attacks

[1]M.YUVARAJ, [2]A.R.BHARATHIDASAN, [3]N.KUMAR

[1, 2] M.E Student, [3]Assistant Professor

[1, 2, 3] Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Tamilnadu, India

[1] yuvaraj426@gmail.com, [2] bharathi.cse09@gmail.com, [3] nkvsc.org@gmail.com

***Abstract*-The inadequacy of login protocols designed to address large scale online dictionary attacks (e.g., from a botnet of hundreds of thousands of nodes). Brute force and dictionary attacks on password-only remote login services are now widespread and emerging technique. Convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. In this paper, we propose a protocol called Password Guessing Resistant Protocol (PGRP), derived upon revisiting recent proposals designed to avoid such attacks. In PGRP limits the total number of login attempts from unknown remote users to as low as a single attempt per username, the users in most cases (e.g., when attempts are made from known, frequently-used machines) can make multiple failed login attempts before being challenged with an ATT. We evaluate the performance of PGRP with two real-world data sets and find out more than the existing proposals.**

***Key Terms*- Online Attacks, Brute force, ATT, PGRP**

Full Text: http://www.ijcsmc.com/docs/papers/February2014/V3I2201499a22.pdf