A countermeasure algorithm for password guessing attacks

Adesina S. Sodiya*

Department of Computer Science,
University of Agriculture,
P.M.B. 2240, Abeokuta, Ogun State, Nigeria
E-mail: sodiyaas@unaab.edu.ng
E-mail: sinaronkei@yahoo.co.uk
*Corresponding author

A.A. Afolorunso

School of Science and Technology,
National Open University of Nigeria,
14 – 16, Ahmadu Bello Way, Victoria Island, Lagos, Nigeria
E-mail: releafolorunso@yahoo.com

Omoniyi P. Ogunderu

Department of Computer Science,
University of Agriculture,
P.M.B. 2240, Abeokuta, Ogun State, Nigeria
E-mail: omoniyiogunderu@yahoo.com

Abstract: Password authentication systems, which are used as first level of defence, are not efficient enough to withstand the dynamic techniques of attackers. In this work, an authentication scheme using first trial protocol (FTR protocol) was developed to prevent dictionary and brute force attacks. FTR protocol uses a rule-based reasoning and splits the process of authentication into two layers; first and second layer protocols. The first layer undertakes the validation of the login password against set of recorded invalid passwords in the first layer repository. The second layer is the second line of authentication in another host different from that of first layer containing the protocol and its penalties. 11,000,000 human authentication request data were used to conduct an evaluation experiment. Zero vulnerability was found in the protocol and an efficient value of 97.89% was established as a confidence measure. This shows that the protocol is secured against online password guessing attacks.