THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATIONS
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

A Secured Protocol For Preventing Online Dictionary Attack

Onashoga, S. Adebukola and Akinwale, A. Taofik

Dept. of Computer Science, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria

Corresponding Author: bookyy2k@yahoo.com

ABSTRACT

The use of passwords is a major point of vulnerablility in computer security as passwords are often easy to guess by automated programs running dictionary attacks. Several attempts have been made by researchers in order to counter online dictionary attack but with one drawback or the other, for example storing passwords in plain text, denial of service and so on. This paper employs Diffie-Hellman Key Exchange Scheme to impose more challenges to the attackers with three guesses as against one in the referenced protocol. Two way hash functions were used to generate two indices which were encrypted so that the attackers would not be able to compromise with the Server. The new scheme requires a high computatioal time of 1.743years as against 1.6625years proposed by other researchers for discouraging online dictionary attacks.

Keywords: authentication, identification, hash functions, online dictionary attacks, disrcete logarithm theorem.