

Title: A Non-Exchanged Password Scheme for Password-Based Authentication in Client-Server Systems

Author: Shakir M. Hussain and Hussein Al-Bahadili

Source: American Journal of Applied Sciences 5(12): 1630-1634 , 2008

Abstract: The password-based authentication is widely used in client-server systems. This research presents a non-exchanged password scheme for password-based authentication. This scheme constructs a Digital Signature (DS) that is derived from the user password. The digital signature is then exchanged instead of the password itself for the purpose of authentication. Therefore, we refer to it as a Password-Based Digital Signature (PBDS) scheme. It consists of three phases, in the first phase a password-based Permutation (P) is computed using the Key-Based Random Permutation (KBRP) method. The second phase utilizes P to derive a Key (K) using the Password-Based Key Derivation (PBKD) algorithm. The third phase uses P and K to generate the exchanged DS. The scheme has a number of features that shows its advantages over password authentication approaches.