

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

¹ Shakir M. Hussain, ² Hussein Al-Bahadili

¹ Faculty of IT, Applied Science University,
PO Box 22, Amman 11931, Jordan, and

² Faculty of Information Systems and Technology
Arab Academy for Banking and Financial Sciences
P.O. Box 13190, Amman 11942, Jordan

Abstract: The password-based authentication is widely used in client-server systems. This paper 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 other password authentication approaches.
