© 2013 FIZ Karlsruhe

io-port 05967774

Hao, Feng; Ryan, Peter Y.A.

Password authenticated key exchange by juggling.

Christianson, Bruce (ed.) et al., Security protocols XVI. 16th international workshop, Cambridge, UK, April 16–18, 2008. Revised selected papers. Berlin: Springer (ISBN 978-3-642-22136-1/pbk). Lecture Notes in Computer Science 6615, 159-171 (2011).

Summary: Password-Authenticated Key Exchange (PAKE) studies how to establish secure communication between two remote parties solely based on their shared password, without requiring a Public Key Infrastructure (PKI). Despite extensive research in the past decade, this problem remains unsolved. Patent has been one of the biggest brakes in deploying PAKE solutions in practice. Besides, even for the patented schemes like EKE and SPEKE, their security is only heuristic; researchers have reported some subtle but worrying security issues. In this paper, we propose to tackle this problem using an approach different from all past solutions. Our protocol, Password Authenticated Key Exchange by Juggling (J-PAKE), achieves mutual authentication in two steps: first, two parties send ephemeral public keys to each other; second, they encrypt the shared password by juggling the public keys in a verifiable way. The first use of such a juggling technique was seen in solving the Dining Cryptographers problem in 2006. Here, we apply it to solve the PAKE problem, and show that the protocol is zero-knowledge as it reveals nothing except one-bit information: whether the supplied passwords at two sides are the same. With clear advantages in security, our scheme has comparable efficiency to the EKE and SPEKE protocols.

Keywords: Password-Authenticated Key Exchange; EKE; SPEKE; key agreement
doi:10.1007/978-3-642-22137-8_23