Cryptology ePrint Archive: Report 2013/058

Cryptanalysis of the Dragonfly Key Exchange Protocol

Dylan Clarke and Feng Hao

Abstract: Dragonfly is a password authenticated key exchange protocol that has been submitted to the Internet Engineering Task Force as a candidate standard for general internet use. We analyzed the security of this protocol and devised an attack that is capable of extracting both the session key and password from an honest party. This attack was then implemented and experiments were performed to determine the time-scale required to successfully complete the attack.

Category / Keywords: cryptographic protocols / cryptanalysis, password authenticated key exchange

Date: received 5 Feb 2013

Contact author: dylan clarke at ncl ac uk