Cryptology ePrint Archive: Report 2011/070

Rational authentication protocols

Long H. Nguyen

Abstract: We use ideas from game theory to transform two families of authentication protocols so that even an intruder attacks a protocol, its payoff will still be lower than when it does not. This is particularly useful in resisting or discouraging a powerful and rational intruder (as present in military applications) who makes many attempts to break a protocol because (1) even the intruder fails, a denial of service attack is still mounted successfully, and (2) in a password-based protocol, the chance of a successful attack increases quite significantly as more and more attempts are launched to guess the password.

Category / Keywords: cryptographic protocols /

Publication Info: game theory, authentication protocol

Date: received 10 Feb 2011

Contact author: Not published