Abstract

A One-Time Password Authentication Method

Takasuke TSUJI

Applications for transferring money or personal information are increasingly common on the Internet and in mobile communications. These applications require user authentication for confirming legal users. One-time password authentication methods change the verifier every time by sending the present verifier along with the next verifier. However, such methods risk attacks because those protocols use two verifiers every session. The SAS (Simple And Secure password authentication protocol) is a one-time password authentication method that uses a hash function five times, but it requires high overhead on low spec machines. In this paper, I propose a new method, SAS-2, which reduces hash function adaptation overhead by 40%. This method has a mutual authentication phase which maintains synchronous data communications in its authentication procedure. Moreover, SAS-2 can be applied to key-free systems.

key words cryptography, hash function, one-way function, password authentication, one-time password