Abstract

This paper presents the implementation of an interactive Zero Knowledge Password authentication scheme for commercial Web sites. In this scheme, a legitimate prover (client) can exchange a secret code (password) with a remote skeptic (server), in order to reveal his/her identification. Based on the validity of the secret code the skeptic then allows the prover to login to the site and access the web services. This paper introduces a protocol that integrates the concepts of Discrete Logarithm Problem (DLP) and Zero-Knowledge Proofs (ZKP). The protocol consists of three entities, namely, the prover, the skeptic, and the facilitator who interact with one another to generate the secret code. When tested, the time to carry out various operations related to this protocol was reasonably small (under 4 seconds). Our scheme is resistant to man-in-the-middle attack and discourages replaying previously intercepted secret codes. We also propose two modifications to our basic scheme to make it resistant against the attack on Integrity and Denial of Service attack (DOS).
References


Index Terms

Computer Science

Algorithms

Keywords

Discrete Logarithm Problem (DLP), Zero-Knowledge Proofs (ZKP), Dynamic on-Demand
Password (DDP), Authentication, commercial web sites and Denial of Service (DOS) attack