

عنوان مقاله:

A light weight authentication and key agreement protocol for grid systems

محل انتشار:

هفتمین کنفرانس ملی مهندسی برق و الکترونیک ایران (سال: 1394)

تعداد صفحات اصل مقاله: 5

نویسندگان:

Saeide Nemati - Nonprofit institution of Taali Qom, Iran

A Rasouli - Nonprofit institution of Taali Qom, Iran

خلاصه مقاله:

Grid computing provides high computing power enormous data storage, and collaboration possibilities to its users. In the networked access to the computational and data resources, security plays an important role. Trust relationships among the communicating entities and faster access to resources are a major concern. Many researchers have proposed security protocols for grid system security based on Public Key Infrastructure (PKI), which needs too much computing resources and time. Moreover, While the number of grid users is exploding, grid administrators are facing a real concern in securely distributing and managing users' credentials and revoking the compromised ones. Few researchers have proposed grid security protocols without public key settings, which reduces huge computation processes but prone to malicious attacks. In this paper we will propose an authentication and key agreement protocol using light cryptographic operations like hash, XOR, etc, which resists major cryptographic attacks and provides mutual authentication and secure key agreement among the entities involved.

کلمات کلیدی:

grid security, authentication, key agreement, certificateless, light weight cryptography

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/459473>

