Abstract

Today almost all organizations in the world are network-centric paradigm and to safeguard the data in a world where technology is advancing, systems are changing rapidly and information flows freely requires efficient secure channel at the endpoint. Security is the heart of IT revolution and more specifically user authentication and key establishment are the rudimentary services in secure communications. Though many systems, schemes bank on public key digital certificate user authentication and key establishment, failed in getting authenticated due to some forgery attacks. Public key Digital certificate though gained popularity in the public key infrastructure (PKI) in providing authentication to user public key, itself cannot be used to
safeguard an authenticate user. In this paper, we propose a novel approach using GDC for user authentication and key establishment. A GDC is a kind of Digital Certificate which contains user's public information and Digital signature which is issued and signed by the trusted Certificate Authority. The advantage of GDC is that, unlike the public key Digital Certificate, it does not contain user's public key. So, the digital signature can never be revealed to the verifier and this is where a digital signature of GDC becomes a security factor that can be used for user authentication. Using this phenomenon, we have implemented a Discrete Logarithm Protocol which satisfies in achieving user authentication and secret key establishment. In addition to this, by using the shared-secret key, we have also exchanged the data between the entities through AES (Advanced Encryption Standard) Cryptographic algorithm.

References

- en.wikipedia.org/wiki/Discrete-logarithm

Index Terms

Computer Science

Security

Keywords
Generalized digital certificate  user authentication  key establishment
shared-secret key

forgery attacks

data exchange (encryption and decryption).