{tag} {/tag}

International Journal of Computer Applications

Volume 96 - Number 22

Year of Publication: 2014

Authors:

M. V. Kishore

G. Pandit Samuel

N. Aditya Sundar

M. Enayath Ali

Y. Lalitha Varma

10.5120/16924-6762

{bibtex}pxc3896762.bib{/bibtex}

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

- L. Harn and J. Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", IEEE trans. on Wireless Communications, vol. 10,pp. 2372-2379,2011.
- Bismin. V. Sherif and Andrews Jose, "Secure Communication using Generalized Digital Certificate", International Journal of Computer Applications Technology and Research, Volume 2-Issue 4,396-399,2013.
- Network Working Group, "Internet X. 509 Public key Infrastructure Certificate and crl profile, RFC:2459," Jan 1999.
- D. Chaum and H. van Antwerpen, "Undeniable Signatures," Advances in Cryptology-Crpyto'89, Lecture Notes in Computer Science, vol. 435, pp. 212-217, 1989.
- R. Rivest, A. Shamir, L. Adleman, "A method for obtaining Digital Signatures and Public-Key Cryptosystems," Commun. Assoc. Comp. Mach. , Vol. 21, no. 2, pp. 120-126, 1978.
- T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE. Trans. Inf. Theory, vol. 30, no. 24,pp. 469-42, 1985.
- L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discrete logarithm, "Electron. Lett. , vol. 30, no. 24. pp. 2025-2026, 1994.
- 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).