Abstract

Kerberos is a network authentication protocol & is designed to provide strong authentication for client/server applications by using secret-key cryptography. Our research was aimed at enhancing the security of transactions over a network. In this paper, we used Kerberos Encryption Technique for authentication and transaction security in the network. Further, we
created an Authentication Server that used to derive a 64 bit key from user’s password. This password was of arbitrary length. The generated key then was used by authentication server, to encrypt ticket granting ticket + session key. The key generated by authentication server was then used by the client at the time of transaction through the transaction server to validate an authentic transaction. However, there was an issue of cross-validation of the ticket by the transaction server for which we included a database and encryption of all the text sent by any client to the transaction server.

Reference

- Steve Mallard(2010), “Methods of authentication”, Bright Hub
- “How Kerberos Authentication Works”, Network on line magazine, Jan 2008
- “How Kerberos Authentication Works”,Learn Networking on line magazine, Jan’2008
- Frederick Butler,, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov and Christopher Walstad, “Formal Analysis of Kerberos 5”, Sep 2006
- Ravi Ganesan, “Yaksha’ : Augmenting Kerberos with Public Key cryptography”.
- Chris Brenton with Cameron hunt , “ ACTIVE DEFENCE A comprehensive guide to network security”

Index Terms

Computer Science
Pattern Recognition
Key words
secret key
Local Directional Pattern
cryptography
authentication
ticket
session key