ABSTRACT

Many organizations have growing mobile users who access resources, and acquire information remotely from portable devices. Hence, there is the need to implement a strong authentication and authorization technique, which can safeguard user credentials and have strict control on the user’s access rights to critical services. We analyzed and found that Kerberos is a strong protocol, which can support Authentication and resource access requirements.

Kerberos performs authentication by using a conventional secret key system, which uses password based encryption. This makes it vulnerable to various attacks. To address these issues we have proposed a secure authentication system based on a public key system which doesn’t use password, and which is lighter on computation and network traffic. Customization is done to authentication phase of Kerberos where client authenticates to the ticket granting server. Device key is used for encryption of timestamp, eliminating the need of public key for authentication.

In this research enhancements are proposed to the Kerberos protocol by using asymmetric key cryptography and the context-aware access control mechanism. This combined symmetric and asymmetric approach reduces communication and computational overheads of the Key Distribution Centre (KDC) server during authentication. By building a customized dynamic authorization mechanism in the second phase of Kerberos, it reduces the total number of messages between the client and the KDC. A novel approach called
the Public Key Context-aware Kerberos system is introduced here. This novel approach extends Kerberos, and adds a new security layer of protection for authentication and authorization phases.

The primary goal is to enhance the authentication and authorization phases of the Kerberos protocol using asymmetric key cryptography and the context-aware access control mechanism.

The approach is to design a Public Key Location-aware Kerberos (PKLK) system which addresses the security needs of mobile users by modifying the Kerberos and using dynamic context aware information i.e., location of the user and also to reduce computational and communication overheads.

Result analysis shows that in authentication, we could reduce the bytes transferred between the client and server, to approximately one third of the well-known PKI based Authentication system. Enhancing Authorization Capabilities by allowing dynamic context based decisions before sharing service tickets in authorization, results in scalability.