Chapter 1

INTRODUCTION
Chapter 1: INTRODUCTION

1. Introduction

1.1 Background

1.2 Kerberos Authentication Protocol

1.2.1 The Features of Kerberos Authentication Protocol

1.3 Analysis of Kerberos Authentication Protocol

1.4 Motivation

1.5 Problem Statement and Methodology

1.6 Objectives

1.7 Statement of Scope

1.8 Efficiency Issues and Solving Approach

1.8.1 Operation of system

1.8.2 Addressing Efficiency Issues:

1.9 Organization of the Thesis
Chapter 1
INTRODUCTION

Authentication plays vital role in the field of information and computer system. The operation on the system cannot be allowed without correct knowledge of the entity. After providing proper credentials, only the system should authenticate the user. Conventional authentication systems are not appropriate where intruder or attacker can capture the password by monitoring network traffic by any other means. In these scenarios strong authentication system is necessary.

Today many organizations, offices, IT services and companies use open and distributed architectures. In general, dedicated work stations and centralized or distributed servers are the components of distributed system. In this environment the user needs to prove an identity for every service requested and in response servers also need to prove their identity. The process in which user’s identity is verified is called authentication.

Many organizations use mobile computing technology to carry out their business operations which provide lot of benefits such as follows:

- Get real-time access to critical information and the applications from any location for efficient decision making.
- Improves operational efficiency.
- Improvements in communications from any location.
- Speeds up business transactions.
• Increases individual productivity and reduces intermediate staff.
• Gives faster access to information, and results in productive output in less time.
• Improves customer relations.

Mobile users usually, want to stay connected throughout the day by logging through their Laptop once. A complex password is a burden on them to memorize and they usually hate to re-enter the password again and again. So, they end up keeping a simple password and it makes the hacker’s job easy. Organizations are providing access to critical information to the mobile users to remain competitive in the market. Mobile users need to access resources on demand from any location. Hence, organizations are worried about information being carried out from a secured area to unsecured zones. In such a challenging environment the important and critical resources of organization need to be protected by administrator.

1.1 Background

Authentication is the assurance of communication entity that it is same one who claims to be. Authentication of an entity is generally done by the evidence it holds. Evidence may include username and password or other means such as finger print, retina scan, voice recognition, smart card and many more [1].

The authorization comes after authentication. The important functionality of authorization is to find out whether a particular user is
permitted to perform a particular operation on object after logging to system or service [2]. Authorization is allowed based upon the restriction parameter. Restriction parameters include physical location restriction, time of day restriction, and multiple access restriction and so on [3]. For example, consider logging into medical hospital system. You may be authorized to see the names of patient and their ward number, but based upon the authorization provided, you may not be allowed to see the payroll information of employee or medical information of patients.

An access control model based upon contextual information incorporates the context information in controlling access to sensitive resources [4]. It acquires contextual information from the corresponding context providers and then feeds it to the authorization decision engine that evaluates the contextual information against the corresponding access control policies to produce an access control decision [5].

A majority of authentication and authorization solutions, which are popular in the market, are either dependent on a password, a smart card or a token or combinations of these, but none is considering dynamic data like the user’s location. Now a days due to devices like Smart phones, Global Positioning System (GPS), and networks it’s becoming possible to use dynamic information as an additional factor before an access is provided to the user [6]. This work is to design a protocol, which can strongly and securely support the above needs authentication and authorization [7].
Kerberos is an authentication protocol used in a computer network [8]. It is used to prove the identities of two parties to each other in a secure manner over non-secure networks [9]. Client (user) and server mutually authenticate to each other by verifying individual identities. Kerberos is a ticket based authentication system [10][11]. Kerberos Authentication protocol is based upon symmetric key cryptosystem. Kerberos uses centralized server called Key distribution server (KDC) whose function is to authenticate client and server to each other [12].

Public-key crypto system includes cryptographic algorithms generating two separate keys [13]. One key is called as secret key and can be by the user. This key is not exchanged or shared with other user. Other key is called as public key. This key is shared with other users publically. These two keys are mathematically linked. One key is used for encryption or locking then other respective key can only be used for decryption or unlocking [14][15]. Public key is shared without compromising the security of system and private key must not be made public.

1.2. Kerberos Authentication Protocol

Kerberos is authentication protocol developed at MIT as part of project Athena. Kerberos is proved and widely used authentication system. It is deployed in many operating and networking systems as authentication protocol. Kerberos has replaced Network LAN Manager (NTLM) as the default authentication protocol in an Active Directory of Microsoft based single sign-
on method. Windows Active Directory implementations include Kerberos as part of authentication system [16]. Oracle Advanced Security replaces traditional password based authentication to strong authentication solutions based on Kerberos and Public key infrastructure (PKI). The IBM Version of Kerberos is referred to as IBM Network Authentication Service (IBM NAS). IBM NAS for AIX supports both the Kerberos client and the Kerberos server. To provide the support for Single Sign-On (SSO) Mac OS X includes Kerberos, the open-source SSO authentication protocol [17][18] for security critical and important data and passwords.

Kerberos Version 5 was standardized and is used in universities, educational institutions, government, military and business. Kerberos authentication protocol is a ticket-based system relying on symmetric key cryptography [19]. The two components, Authentication Server (AS) and Ticket granting server (TGS) performing the functionality of creating and distributing the tickets to the entity upon receiving the request [20]. Kerberos uses strong symmetric cryptography to achieve authentication over insecure network. All the operations in the standard Kerberos including communication between AS, TGS and Application servers are based on symmetric key cryptography. As it works on symmetric key, the secret key (e.g. password) is shared between the server and client [21]. Naturally, it raises the risk of various attacks like password guessing, brute force, and dictionary attack [22]. Using public-key cryptography which relies on two keys, it prevents all attacks like password
guessing, shoulder sniffing, brute force and dictionary attack related to user password. It also simplifies key management making it scalable [23].

Kerberos authentication protocol schematic is as shown in Figure 1.1

Fig.1.1: Kerberos Authentication Protocol.

Components of Kerberos Authentication protocol:

- Key distribution centre: Stores cryptographic keys (secret keys), Supports authentication services, responsible for creation and distribution of session keys.
- Authentication service: It is a component of the KDC which actually provides the functionality authentication.
• Principals: All entities that are used by the Kerberos are identified as principals; it includes users, services, applications or resources.

• Realm: The logically grouped set of principles by an administrator is called as realm. A KDC may create one or more realms of principals.

• Ticket granting service: TGS is part of the KDC which is responsible for creating and distributing tickets to the principles, tickets contain session keys.

• Ticket: A token used for authentication [24].

A. Authentication (AS_Exchange) phase: This is also called as the Logon phase. Client sends an authentication request to the server and obtains credentials Ticket Granting Ticket and the session key [25]. Client message consists of Identification of Clients, Identification of Ticket granting server and Time stamp. After receiving the request from client, authentication server relies with message. Message consists of Keys shared between client and TGS, Identification of TGS, Time stamp, lifetime and Tickets. All these fields are encrypted with key which is known to Client and TGS only as stated below.

Details of exchanges in Authentication phase

CAS: ID_c || ID_TGS || TS_1

ASC: E_{K_c[K_c,TGS || ID_TGS || TS_2 || Lifetime_2 || Ticket_{tgs}}

Ticket_{tgs}=E_{ktgs[K_c,TGS || ID_c || AD_c || ID_{tgs} || TS_2 || Lifetime_2}}

Figure 1.2 depicts Steps 1 and 2 in the request AS_REQ and response AS_REP.
B. Authorization (TGS_Exchange) phase: After obtaining TGT from step 2 the client sends an authorization request for a specific service and obtains a service granting ticket (SGT) and a newly created session key [26].

Details of exchanges in Authorization phase

CTGS: ID_v | Ticket_{tgs} | Authenticator_c

TGSC: E_{K_c,tgs}[K_c,v | ID_v | TS_4 | Ticket_v]

Ticket_{tgs}=E_{tgs}[K_{c,TGS} | ID_c | AD_c | ID_{tg_s} | TS_2 | Lifetime_2]

Ticket_{tv}=E_{kv}[K_{c,v} | ID_c | AD_c | ID_v | TS_4 | Lifetime_4]

Authenticator_c=E_{K_c,tgs}[ID_c | AD_c | TS_3]
Steps 3 and 4 in Figure 1.3 depict request TGS_REQ and response TGS_REP in the authorization phase.

![Kerberos TGS Service Exchange](image)

**Fig.1.3: Kerberos TGS Service Exchange.**

**C. Access to Application Server (AP_Exchange) Phase:** This phase starts with the client sending an access request for service to the target application server using SGT and session key acquired in the authorization phase. The application server validates the request and sends an acknowledgement to the client.

**Details of exchanges in Application server Phase**

CV: Ticket$_v$ | Authenticator$_c$

VC: $E_{KC,v}[TS_5+1]$
$\text{Ticket}_v = E_{kv}[K_{c,v} \mid \mid ID_c \mid \mid AD_c \mid \mid ID_v \mid \mid TS_4 \mid \mid \text{Lifetime}_4]$

$\text{Authenticator}_c = E_{kc,tgs}[ID_c \mid \mid AD_c \mid \mid TS_3]$

Steps 5 and 6 in Figure 1.4 depict request AP_REQ and response AP_REP.

**Fig. 1.4: Kerberos Application Service Exchange.**

1.2.1 The Features of Kerberos Authentication Protocol:

Kerberos supports authentication but has little support for authorization. Functionality like digital signatures is also not supported by Kerberos. Public key cryptosystem for initial authentication as well as cross realm authentication have been proposed but they don’t scale.
Some of the features of Kerberos authentication protocol are as follows:

- It integrates cleanly with OpenLDAP. Integration with Kerberos is via the Simple Authentication and Security Layer (SASL)/Generic Security Services Application Program Interface (GSSAPI) authentication mechanism.
- Kerberos is scalable and has been proven to support thousands of users. Problems like failover and load balancing can be addressed by replicating KDC [27].
- Integrity and confidentiality can be supported by The GSSAPI in Kerberos.
- Functionality of Single sign-on is supported by Kerberos Authentication protocol [28].
- GSSAPI authentication is supported by protocols and applications, hence it can be used with Kerberos [29] [30].

Kerberos has a number of limitations. It is decided to enhance it in such a way that it will suit the mobile users giving flexibility and still having a mechanism where the organization can control “user access” dynamically, and reduce vulnerabilities related to “password hacking” [31][32].

1.3 Analysis of Kerberos Authentication Protocol
Despite Kerberos’ many strengths, it also has some weaknesses and limitations as below:

• Kerberos works on symmetric key. The Kerberos server stores the user’s id and passwords. There is a fair possibility that by gaining access to the Kerberos database an attacker can get unauthorized access [33].

• Kerberos supports only coarse-grained authorization. It does not have a strong validation or rejection mechanism while providing Service Tickets to the user [34].

• Single point of failure: Continuous availability of a central server is basic requirement in Kerberos. Services cannot be availed when Kerberos server is down.

• Time synchronization: The clock of involved hosts must be synchronized within the configured limits. Kerberos has strict time requirements. The authentication will fail if the host clock is not synchronized with the Kerberos server clock [35] [36].

1.4 Motivation:

In the context of computer security, the user authentication is basic building block. Authentication of a particular entity is done by verifying its credentials. In traditional system generally these credentials are user name and password. Other types of credentials are also used for authentication. Finger print, retina scan, voice recognition smart card can be used as
credentials for authentication. Showing your identity card for voting to the election officer is equivalent to authentication.

There is a need to develop strong authentication system where only an authorized user should get permission to access protected information. This task becomes ever challenging in mobile computing environment.

The solution can be looked into authentication based upon location as one of the parameter. Location information consists of latitude and longitude. Sometimes altitude is also component of location parameter. Location is associated with GPS receivers like Earthmate, Garminetrex etc. Mobile devices having GPS features can also be used for capturing location information. Authentication system can be improved by adding location information into present security mechanisms.

1.5 Problem statement and methodology

Kerberos performs authentication by using conventional (shared secret key) cryptography, which has some weaknesses. Authentication is the first phase, which is password dependent. It makes the protocol vulnerable from attackers for password hacking using offline or online attacks. To overcome this risk public key cryptography (PKC) is used in the initial authentication of Kerberos. Although PKC strengthens Kerberos in terms of security there are noticeable limitations like computational burden and communication overhead, which impacts KDC. In addition to authorization, which is the second phase of Kerberos, it has few limitations. It provides a service ticket to all valid users
present in the system and expects the application server to take decisions on granting or rejecting user requests in the third phase. Due to this the rejection of an unauthorized user in the third phase, messages passes becomes necessary, which is again an overhead to the system. It introduces the risk of replay attack in the third phase where an attacker can simply reuse the request of the third phase to authenticate himself to a server [37].

To address the above issues we have proposed a password-less secure authentication based on a public key which is lighter on computation and network traffic. We have customized the second phase of Kerberos using the user’s context, e.g. location and provide dynamic access control.

Here, 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 [38]. We have proposed a Public Key based Location-aware Kerberos system to meet the objectives. The basic purpose is to address the issue authentication needs of users.

1.6 Objectives

Here, 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. We have proposed the Public Key Context-aware Kerberos (PKLK) system to meet the below mentioned objectives:

- Address crucial authentication security needs of Mobile Users during
remote login by providing a password-less authentication system.

- Embed Public Key security features into Kerberos.
- Reduce computational and communication overheads of the Authentication phase as compared to the well-known PKI based Authentication systems.
- Develop a context-aware authorization feature for mobile users by embedding context-aware data (like user's location) by enhancing the Kerberos protocol.

1.7 Statement of Scope

Scope of the project is to develop a Kerberos based authentication and authorization system that will give improved security and provide dynamic authorization capabilities. The system should make the user authentication password independent by using a novel approach and at the same time, the system should build functionality, which reduces computational and communication overheads. The system should customize the authorization part of Kerberos, and permit use of user context (e.g. user location).

Major Inputs to the System:

- User principal (user id), public key, private key, and user’s context (location) are important inputs to the system from the end user.
- Active LDAP database consisting of user profiles and services information.

Output from the System:
• User is authenticated successfully without providing a password to the system, where the system shares a Ticket Granting Ticket back to the user.

• User is authorized successfully upon providing a valid context where the system shares a Service Granting Ticket with the user.

1.8 Efficiency Issues and Solving Approach

Kerberos has a clear separation between authentication and authorization, so a phase wise approach is taken to build the enhanced Kerberos system.

1.8.1 Operation of system

Operation of system is divided into two phases

• Authentication phase

• Authorization phase

1. Authentication Phase:

• This phase needs to support password-less authentication, and hence the option of public key cryptography is used for user logon.

• Combined symmetric and asymmetric cryptography is considered for this phase so as to remove password dependency.

• For authentication requests, a symmetric encryption based user’s device key is used. Here password is replaced with device key.

• For authentication response we customized the KDC component to use
public key cryptography while sharing authentication response.

2. Authorization Phase:

• To improve the authorization phase, the Kerberos protocol RFC specifications are studied in detail. This is to identify attributes, which can carry additional payload for authorization from the client to the server and server to client.

• Studied different context parameters associated with the user, which can be used as an input for dynamic validation. User location is selected as a context parameter and embedded in the authorization request.

• A device key is used for encryption and decryption of context data.

1.8.2 Addressing Efficiency Issues:

• This combined symmetric and asymmetric approach reduces the communication and computational overheads of the KDC server.

• By building a customized dynamic authorization mechanism in the second phase of Kerberos, it reduces the total number of messages between the client and KDC.

   Research key outcome is a development of the Public key based location aware Kerberos (PKLK) system based on Kerberos, which gives improved computational and communication efficiency for the authentication phase and provides customized dynamic authorization capability.
This Research gives a comparative analysis of Kerberos, and Public key cryptography for Initial Authentication (PKINIT) and the PKLK system on the following performance parameters:

- Authentication payload (request and response) results
- Computation analysis - number of public and symmetric key operations
- Authorization – number of message exchanges with an illustration

All this qualitative and quantitative analysis is shown by graph and in tables wherever necessary.

1.9 Organization of the Thesis

The thesis is organized in to six chapters. In first chapter introduction of Kerberos authentication protocol is given. Second chapter presents about literature survey. Third chapter discusses about proposed system architecture of Public key based location aware Kerberos protocol. Fourth chapter illustrates experimental setup. Fifth chapter presents the results and discussion. In the sixth chapter conclusion is given.