International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

SECURITY MODEL FOR E-COMMERCE THROUGH AUTHENTICATION USING KERBEROS

Miss. Sweety R. Lodha[1], Prof. S. S. Dhande[2]
[1]Master of Engineering, [2]Guide, Department of Computer Science &Engineering
Sipna College of Engineering & Technology, Amravati, India.

Abstract: E-commerce applications are becoming popular day by day as they are working like a virtual shop. Now a day, E-commerce is very popular way for selling, buying and doing business. E-commerce business operators face many challenges in building consumer trust and in providing e-security for their network. In E-commerce Information Security is very essential measure. E-commerce includes protection of user assets from unauthorized access, use, destruction, or alteration. To protect the user details different methods are used. Replay attack and password attacks are serious issues in the authentication protocol. In this paper we include the method which prevents replay attacks and password attacks by using Triple password scheme of Kerberos. In Triple password scheme of Kerberos, Authentication Server sends two passwords to Ticket Granting Server (one for Application Server and one for TGS) by encrypting it with the symmetric key shared between Authentication server and Ticket Granting server. Ticket Granting Server sends password to Application Server by encrypting with the symmetric key shared between TGS and application server Then Service-Granting-Ticket is transferred to users by encrypting it with the password that Ticket Granting Server just received from Authentication Server. It helps to prevent Replay attack.

Keywords: Kerberos Protocol, Authentication Server, Authorization, Application Server, Ticket Granting Server

I. INTRODUCTION

As an electronic commerce exponentially grows, the number of transactions and number of participants using e-commerce applications has been rapidly increased. Since all the interactions among users occur in an open network, there is a measure risk for sensitive information to be disclosed to unauthorized persons. When the internet connection came into picture then the password oriented authentication was invented. But this current system of authentication is not good enough to ensure the clients safety of personal information. Security problems on the network receive public awareness, and the media carry stories of high-profile harmful attacks via the internet against business, academic sites and government [1].

The Password protected authentication can be easily known by the invader to know the password. And also the client must always remember the password, and enter it each time she wants to login. The attacker can know the password by hit and trail technique [2]. Complicated set of protocols and methods have been created to handle with information security problems. Kerberos is an authentication system that uses symmetric key cryptography to protect sensitive details on an open network. It is a ticket based system in which Kerberos server delivers a ticket encrypted/coded with the user's password when the user logs in. The user decodes the ticket and uses it to obtain tickets for other web services he or she wants to use [3]. To carry out secure authentication, Kerberos uses trusted third party known as Key Distribution Center (KDC) which is made of two components:

- Authentication Server, used to authenticate client.
- Ticket Granting Server, used to grant the ticket.

Kerberos intended to centralize authentication for entire internet—rather than storing precise authentication information at each clients's machine [4][5].

II. LITERATURE REVIEW

A lot of analysis has been worn out on the Kerberos authentication protocol. Kerberos is stateless [6], which enhances scalability. Session keys are not hold by Kerberos servers, but are included in the TGT and SGT so that the client can converse privately with the TGS and application servers. Single sign-on (SSO) is an important concept of Kerberos. With SSO, a client's password must only be entered once per session. The TGT and session key obtained in first phase are saved, so each time the user wants to gain access to a service, only 2nd and 3rd phases are performed. The tickets having start/end times indicating a valid time period when they can be used. SSO provides efficiency, convenience, and added security. Needham and Schroeder [Nee78] proposed that, Kerberos is trusted to hold in confidence symmetric keys known by each client and server on the internet. The key shared with the KDC forms the foundation upon which a client or server trusts the authenticity of the tickets it receives. A Kerberos ticket is valid for a finite period called its lifetime. When the interval ends, the ticket expires; any later authentication exchange needs a new ticket from the KDC [7]. In [8] there is a dialogue that was written in 1988 to help its readers understand the fundamental reasons for why the Kerberos V4 protocol was the way it was. Miller and Neuman are the primary designers of Kerberos Version 4 with contributions from Saltzer and Schiller [9]. They published that version in the late 1980s, although they had targeted it primarily for Project Athena. Version 5, proposed by Kohl and Neuman, appeared as RFC 1510 in 1993 [10], with the aim of overcoming the limitations and security problems of version 4. Boldyreva and Kumar at 2007 take a close look at Kerberos' encryption and comer that most of the options in

the recent version provably provide authenticity and privacy [11]. Kerberos is also used in wireless systems. Erdem proposed a high speed 2G wireless authentication systems based on Kerberos [12]. Kerberos is also introduced to be used in IPv6 networks. Sakane, Okabey, Kamadaz, and Esakix describe a method to establish secure communication using Kerberos in IPv6 networks [13]. Nitin et al. present an image based authentication system using Kerberos protocol at 2008 [14]. Jian [15] proposed an optimized way to avoid password attack and replay attack in SSO system. Multiple databases were added to provide the authorization and authentication in order to prevent replay attack. In this approach, Authentication Server (AS) sends Ticket-Granting-Ticket (TGT) to user as well as to Ticket- Granting-Server (TGS).Similarly; TGS sends Service-Granting-Ticket to Client as well as Application server. TGS and AS, each has their own database. They store these tickets in their database and if attacker replays Ticket-Granting-Ticket (TGT) or Service-Granting-Ticket (SGT), they can easily find out whether this is an attack or not. A dynamic double password based sign-on protocol was proposed [16]. That protocol makes use of two passwords that are needed during the client signup and log files concept was used. Log file contained the details when a particular client visited to a server which could be Authentication Server, Ticket Granting Server or Application Server. Application server generates log file and transfers to AS even after responding the client. Authentication server passes this log file to clients. Therefore, a user can make a judgment on security of password through auditing log files and allowed to changing the password. So, if an attacker has captured a password, client can easily change it by looking and analyzing at the log files. Modified Symbolic Model verifier [17] approach was proposed to discover problems with respect to the replay attack. Location based Kerberos authentication protocol is described in [18]. In this approach server captures P(Y) code off all client in the network and it assigns TGT to the client by encoding (encrypting) session key and TGT with the P(Y) code of user.

After receiving this message, client accepts its P(Y) code using GPS and decrypts the message. So, if an attacker is able to capture the message, then he will not be able to decrypt the message because P(Y) code length is in several of GBs. It will result in the collapse of the ticket due to time synchronization issue. Here, user physical location is added as an additional text into the Kerberos protocol, which helps to find out physical location of the message provider. Server sends TGT to client by encrypting session key with the hash value of user physical location. So, even if an attacker captures a message, he will have to break two phase security to get session ticket and in this process, ticket time may expire. A new protocol for key distribution was proposed [19] after analyzing the security flaws with different protocols that are currently used for the authentication as well as for key distribution. This proposed model is based on using secret keys.

III. PROPOSED METHODOLOGY

The proposed model is designed to advance the authentication process of E-commerce.
It includes the following module:

- Authentication Module
- E-commerce Module

Authentication Module
In proposed method Kerberos authentication module is used to secure user authentication in network.
Kerberos protocol includes following for secure authentication:

- Encryption
- Key Distribution Center
- Authentication Service
- Ticket Granting Service
- Application Service

Encryption
It is the case for all data sent over the network, it can be viewed, modified, tampered. Kerberos provides cryptographic authentication through a combination of symmetric key and strong encryption. This makes sure data confidentiality and message integrity. Here we are using AES encryption mechanism. Symmetric key encryption allows real time authentication because it is a fast mechanism, the same key is used at both end to encrypt and to decrypt the message.

Key Distribution Center
Kerberos protocol is used to authenticate client/principal. A principal can be a simple user, an application server or any other network thing that needs to be authenticated. Three parties are involved in the authentication process:
1) The client/ principal
2) The server/verifier
3)The Kerberos server, i.e. KDC
KDC has two roles: the Authentication Service (AS) and the Ticket Granting Service (TGS). The Authentication Service exchange is done only once between a client and the KDC. The KDC then delivers a Ticket Granting Ticket (TGT) through the TGS, that the client will prefer to obtain more tickets. If the principal wishes to connect to multiple application servers, it will authenticate only single time to the KDC. Then it will use the TGT he obtained to request further tickets to each application server, through the ticket granting service (TGS).

Authentication Service
The primary role of the KDC is the Authentication Service (AS). The client initially requests a ticket to the KDC by specifying its name, an expiry time until when the authentication will remain valid, the service required TGS. The KDC, if it finds the client in its database, replies with two things:

- A user ticket containing a session key and TGS service name and the expiration time, all encrypted

with the symmetric key of the client.

- A granting ticket containing the client's name, a session key and the expiration time all encrypted with the symmetric key of the KDC. This is what is known as the Ticket Granting Ticket. The client, unable to decode the TGT, will use it later to request tickets to other services. As it is encrypted, the principal can't read the data inside. If he tries to change it, the KDC will not be able to decrypt it and it will be rejected.

Ticket Granting Service

The second role of the KDC is to issue tickets; it is called the Ticket Granting Service (TGS). It doesn't query the application server directly. This request to the KDC having many fields:

- An authenticator composed of: a timestamp and a checksum encrypted with the session key, KDC obtained earlier, shared between the principal and the KDC. This proves the principal's identity since he is the one to know this session key. The checksum proves the text wasn't altered while transiting. The timestamp assures the message is recent, and is used to prevent replay attacks. The KDC must reply within five minutes for the message to be accepted. This is why it is important to have good time synchronization across your network when implementing Kerberos authentication.
- The TGT received during the authentication exchange with the KDC. It is used by the KDC to check the principal's name. If the principal name present in the TGT doesn't match with the associated session key. The KDC is unable to decode the authenticator. Also, the KDC verifies the validity of the ticket by checking the expiration time of the authentication.
- The application service server name to which the client wants to establish a connection.
- An expiration time for the Ticket Granting Ticket.

The KDC replies to the principal with two tickets:

- The client ticket containing a new session key that the client and the application server will use to check one another's identity and to encrypt their sessions. The ticket also encloses the expiration time and the application service name of the new ticket. All these items being encrypted with the key, KDC shared between the KDC and the principal, only known to the client.
- The server ticket containing the same session key, the user's name and the expiration time of the ticket. The server ticket being encoded with the application server's symmetric key, only known to the server.

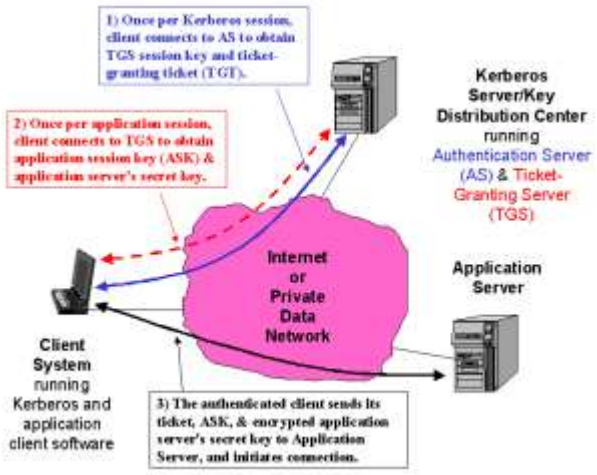

Figure 1: Architecture of Kerberos Authentication

IV. EXPERIMENTAL RESULTS

Figure 2: Sign up screen

When client sign up at that time the whole details get stored in the database. But here the password is encrypted in hashed form that can be decrypted and no one can read it.

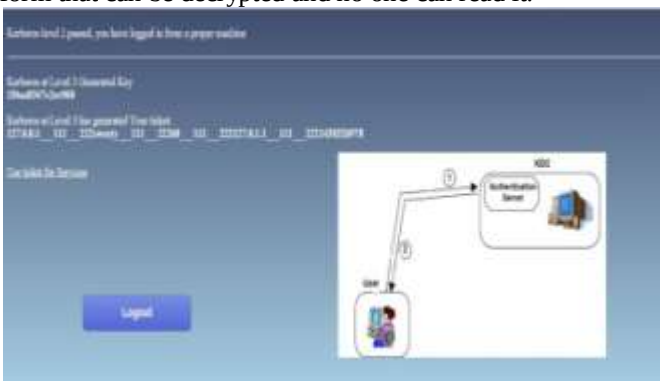

Figure 3: Key and Ticket

When client logs in that time whole details are sent to the Authentication Server of KDC. If client is authenticated then AS sends key which further used with Service Server. Next it sends request to the Ticket Granting Server and receives the ticket which used to communicate with service server. Following fig shows the details that are useful for generating the ticket and lifetime is very important if it gets expired we need to login again.

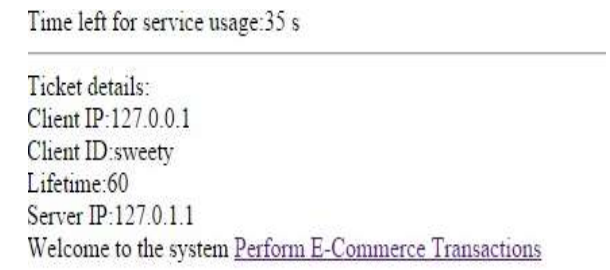

Figure 4: Details used for ticket generation

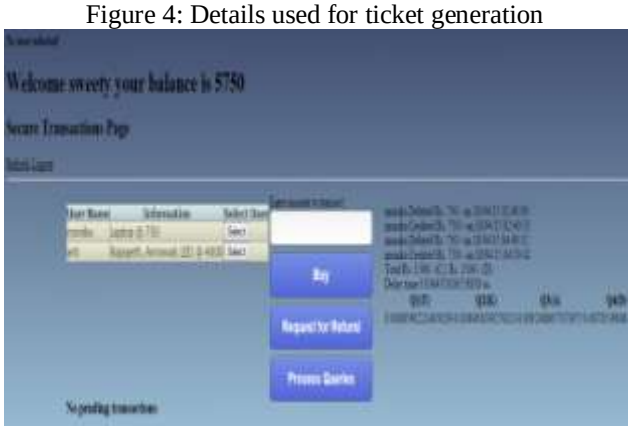

Figure 5: E-commerce module

This is the E-commerce module which contains three options. First two options are present in existing system also but third option shows the all the performed transaction and time taken by the queries to process. Time to process transaction key, key fetch time, amount decode time (which is stored in encrypted form), debit and credit time. Kerberos authentication system requires less time. In this system replay attack is prevented through the three way authentication scheme of the Kerberos. This system is advantageous for authentication and time required to process the queries.

V. CONCLUSION

In this paper, the objective of proposed method is to keep secure the details of the client or principal from the unauthorized access or alteration or destruction. The details of the client are very essential to keep private when using it anywhere. On the E-commerce site if we want to purchase any product we need to register or specify some details so that the required product can be sent properly and transaction is also done securely. In this process there is possibility of replay attack and that attack can be prevented by using the authentication method Kerberos v5. Future work of this system is that the encryption method designed in Kerberos Version 5 is for the secret key encryption; have to use public-key cryptosystems to more secure the communication.

REFERENCES

[1] Oppliger R.,"Security Technologies for the World Wide Web, Second Edition", Library of Congress, ARTECH HOUSE Inc., USA, 2003.
[2] William Stallings,-"Cryptography And Network Security
[3] Sanket Bhat, "KERBEROS: An Authentication Protocol "2014.
[4] Kohl, J. Neuman, C. "The Kerberos Network Authentication Service (V5)", 27 Nov. 2003.
[5] Gagan Dua1, Nitin Gautam2, Dharmendar Sharma3, Ankit Arora, "REPLAY ATTACK PREVENTION IN KERBEROS AUTHENTICATION PROTOCOL USING TRIPLE PASSWORD
[6] A. Harbitter and D. A. Menasc´e. Performance of Public Key-Enabled Kerberos Authentication in Large Networks. In IEEE Conference on Security and Privacy, Oakland, CA,May 2001.
[7] John T. Kohl Digital Equipment Corporation B. Clifford Neuman, "The Evolution of the Kerberos Authentication Service"
[8] B. Bryant, Designing An Authentication System: A Dialogue in Four Scenes, Project Athena document.
[9] Wikipedia, \Kerberos (protocol)," (http://en.wikipedia.org/wiki/Kerberos (protocol))
[10] J. Kohl, and C. Neuman, The Kerberos Network Authentication Service (V5), Network Working Group, RFC 1510, Sep. 1993.
[11] A. Boldyreva, and V. Kumar, \Provable-security analysis of authenticated encryption in Kerberos," IEEE Symposium on Security and Privacy (SP'07),pp. 1-21, May 2007.
[12] M. Erdem, \High-speed ECC based Kerberos authentication protocol for wireless applications," IEEE Global Telecommunications Conference (GLOBECOM), vol. 3, pp. 1440-1444, Dec. 2003.
[13] S. Sakane et al., \Applying Kerberos to the communication environment for information appliances,"IEEE Symposium on Applications and the Internet Workshops (SAINT-w'03), 2003.
[14] Nitin et al., \Security analysis and implementation of JUIT-image based authentication system using Kerberos protocol," Proceedings of the 7th IEEE/ACIS International Conference on Computer and Information Science, pp. 575-580, 2008.
[15] Yang Jian, An Improved Scheme of Single Sign-on Protocol, Fifth International Conference on Information Assurance and Security, PP. 495-498, IEEE 2009
[16] Yang Jian, An Improved Scheme of Single Sign-on Protocol Based on Dynamic Double Password, International Conference on Environmental Science and Information Application Technology, IEEE 2009. PP. 572-575.
[17] Punit Mundra, Shobhit Shukla, Madhavi Sharma, Radhika M Pai and Sanjay Singh, Modeling and Verification of Kerberos Protocol using Symbolic

Model Verifier, International Conference on Communication Systems and Network Technologies, PP 651-654, IEEE 2011

[18] Abdelmajid, N.T., Hossain M.A, Shepherd S, Mahmoud K, Location-Based Kerberos Authentication Protocol, IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust IEEE-2010

[19] Junhong Li, Design of Authentication Protocols Preventing Replay Attacks, 2009 International Conference on Future ioMedical Information Engineering, PP 362-365, IEEE 2009.

