INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# REVIEW ON IMPLEMENTATION OF SECURITY MODEL FOR E-COMMERCE THROUGH AUTHENTICATION USING KERBEROS

**SWEETY LODHA[1], PROF. S. S. DHANDE[2]**

1. Student in Department of Computer Science & Engineering, Sipna College of Engineering and Technology, Amravati.
2. Associate Professor, Department of Computer Science and Engineering, Sipna College of Engineering and Technology, Amravati.

**Accepted Date: 05/03/2015; Published Date: 01/05/2015**

**Abstract:** E-commerce is the one of the way for buying, selling and doing business. E-commerce offers low transaction costs and more suitable business form to all over world consumers and because of that key requirement of E-commerce is to maintain security of business or transaction. To keep this information secure/private there are different asymmetric approaches which use in E-commerce transaction and other supported cryptography algorithms which are essential in working setup of E-commerce. The necessities for securing e-commerce transaction are authentication, privacy, integrity maintenance and non-repudiation. Security problems and risks in E-commerce environment are varied and can be caused intentionally and unintentionally by both insiders and outsiders. Transaction security in business management is the key issue of e-commerce. Replay attack and password attacks are severe issues in the Kerberos authentication protocol. Many ideas have been planned to avoid these attacks but they increase complication of the total Kerberos environment. In this paper we propose an enhanced method which prevents replay attacks and password attacks by using Triple password method. Three passwords are stored on Authentication Server and Authentication Server transfers two passwords to Ticket Granting Server (one for Application Server) by encrypting with the secret key shared between Authentication server and Ticket Granting server. Similarly, Ticket Granting Server transmits one password to Application Server by encrypting with the secret key shared between TGS and application server. Meanwhile, Service-Granting-Ticket is transferred to users by encrypting it with the password that TGS just received from AS. It helps to prevent Replay attack.

**Keywords:** Kerberos Protocol, Authentication Server, Password Attack, Application Server, Ticket Granting Server.

**Corresponding Author: MS. SWEETY LODHA**

**Access Online On:**

www.ijpret.com

**How to Cite This Article:**

Sweety Lodha, IJPRET, 2015; Volume 3 (9): 788-795

*PAPER-QR CODE*

**INTRODUCTION**

With the increased use of Internet Technology, a setup also in existence now that is E-commerce which is based on network and multimedia technology. It controlled transaction through Internet also called open public network which is efficient to implement a different kind of e-business process. E-commerce is an online business. To provide security in the form of E-commerce web service security plays very significant role in such business processes [1]. In E-commerce, growingly increasing security issues need to consider on the open Internet like credit card clowning, client information leakage, etc. [2]. So, it is the cause that people's interest towards using of E-commerce decreasing day by day. To develop the E-commerce, security is an important issue on the Internet. Authentication is a way of ensuring that nobody can access the system without providing the way that proves he has access right. Therefore, rather than each server check request for services, Kerberos is having a central server which does the task of authentication. If an authenticated user acquires access to the resources, he may either gain access to private information or may spoil resources such as Information stored in the database. Therefore, security is required at all places in today world from protecting computer resources to the protection of a nation. But security involves implementation of events to protect attacks. But it does not mean that an attack will never occur. For example, preventing an outside attacks doesn't mean that you are safe/secure; attacks can arise from inside of organization. Therefore, it is essential to provide security inside of an organization. Authentication protocol is one of the most classical single sign-on protocols. A single sign-on system means that a user can have access to all services from the application servers after only sign on single time in a multiple application systems. Kerberos V5 is being used presently but there are lots of replay and password attack issues in it [9]. Kerberos V5 was designed to overcome some of the drawbacks of Kerberos V4, but it can't guarantee to avoid replay and password attack. This paper provides triple layer of security. If an attacker successes in gaining access to the ticket-granting-ticket and obtaining Ticket-granting-service from Ticket Granting Server, he will not be able to perform replay attack because authentication server will request the Ticket-Granting-Service provider about the password. Following figure shows the Kerberos authentication:

- The client and authentication server authenticate themselves to each other.
- The client and ticket-granting server authenticate themselves to each other.
- The client and requested service authenticate themselves to each other, at which point the service will be provided to the client.

Authentication process of Kerberos:

1. The user provides username and password on the client machine, which is cryptographically hashed to form the secret key from the client.

2. The client contacts the Authentication Server, which replies with the following items:

- The client-TGS session key, $K_{CT}$, encrypted using the client's secret key, $K_C$.

- The ticket-granting ticket, encrypted with the secret key of the TGS, $K_T$. The TGT includes key $K_{CT}$ and validity period.

3. The client decrypts the TGS session key $K_{CT}$ using $K_C$. To request a service, the client sends the following two messages to the TGS:

- The TGT and the name, S, of the service being requested.

- An authentication token consisting of the client ID and time stamp, encrypted using the client-TGS session key $K_{CT.}$

4. The TGS decrypts the TGT using $K_T$, thus retrieving the client-TGS session key $K_{CT}$ and the validity period of the TGT. If the current time is within the validity period, the TGS decrypts the authentication token with key $K_{CT}$ and sends two messages to the client:

- A new client-server session key, $K_{CS}$, encrypted with $K_{CT}$.

- A client-to-server ticket encrypted using the specific service's secret key, $K_S$, which is known to the TGS. This ticket contains the client ID, network address, validity period, and key $K_{CS.}$

5. After decrypting the client-server session key $K_{CS}$, the client authenticates itself to service S by sending the following two messages:

- The client-to-server ticket, sent by the TGS in the previous step.

- The client ID and time stamp, encrypted with $K_{CS.}$

6. The service decrypts the client-to-server ticket using its secret key $K_S$ and obtains the client-server session key $K_{CS}$. Using $K_{CS,}$ it decrypts the client ID and time stamp. Finally, to prove its identity to the client, it increments the time stamp by 1 and sends it back to the client re-encrypted with $K_{CS}$.

7. The client decrypts and verifies this response using $K_{CS}$. If the verification succeeds, the client-server session can begin.

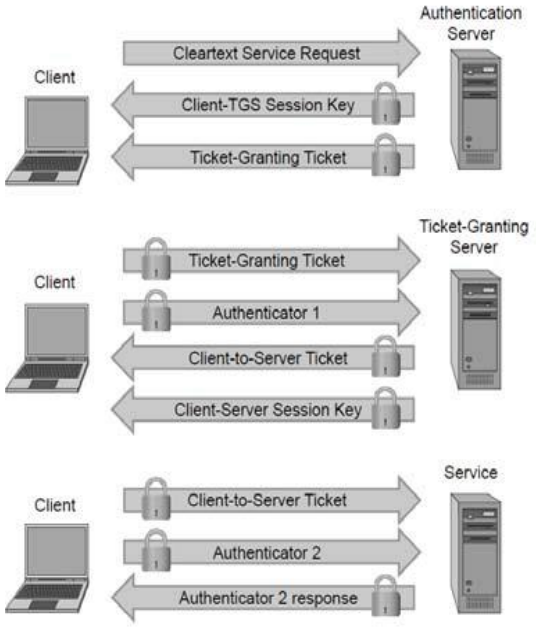


**Figure 1 Authentication process of Kerberos**

## ANALYSIS OF PROBLEM

E-commerce is the electronic commerce which is basically build for doing business from any place to anywhere in the world. This system is liked by various people because the people who were not having time to buy the things by wondering in market they can purchase it online by sitting at their home. But there are some problems occur in account when peoples are using E-commerce. When people do online shopping they need to do payment for that product. To do payment consumer need to use his bank details to transfer the money to E-commerce site. Here is the major problem to maintain the bank details and personal details of the consumer. So to keep the information private is the objective of the E-commerce system. For that different techniques like asymmetric encryption/decryption, user authentication and different security protocols are used. But still to improve the size, time, key memory usage need to build another system that also provides all security mechanism with extra features [10].

E–Commerce business transactions are the security issue that available in two aspects which are the security of the system and security of information. The security of casual can be

tempering with and loss information, denial and forgery information etc. the security issues of system may be damaging, hacking of system with virus activities and so on.

There are many points of vulnerabilities or failure in an e-commerce environment. Even in a simplified e-commerce situation – an only user contacts a single web site, and then enters his credit card and address information for shipping a purchase product – many potential security susceptibilities exist [11]. Indeed, even in this simple scenario, there are a many systems and networks involved. Each has security issues:

- A user must use a web site and at some point authenticate, or identify, him to the site. Typically, authentication begins on the user's personal computer and its browser. Unfortunately, security issues in personal computers offer hackers other ways to steal e-commerce information and identification data from customers. Some recent examples include a popular home-banking system that saves a user's account number in a web cookie which hostile web-sites can break; lack of encryption for home wireless networks and, mail-borne viruses that can steal the user's financial information from the user's keystrokes. While these particular securities problems will be fixed by some software programmers and web-site administrators, similar problems will continue to occur.

- The user's web browser connects to the merchant front-end. When a customer makes an online purchase, the merchant's web-server usually caches the order's personal data in documents of recent orders. This document contains everything necessary for credit-card fraud.

- The merchant back-end and database. A site's servers can damage the company's internal network. This not easily remedied, because the web servers requires administrative connections to the internal network, but web server software tends to have buggy security. The cost of failure is very high, with potential theft of consumers' identities or industrial information. Additionally, the back-end may connect with third party fulfillment centers and other processing agents.

This is a simplified model of e-commerce architecture; yet even in its simplicity, there are many security issues. Note that encrypted e-commerce connections do little to help solve any but network security problems. While other problems might be improved by encryption, there are still vulnerabilities in the software clients and servers that must use the data [12].

Now, we need to solve this problem by providing strong authentication method.

**PROPOSED WORK**

In the proposed model we are trying to advance the process of E-commerce transaction by improving the authentication mechanism. For that we are using the concept of Kerberos.

In the proposed model following activities are going to be performed:

- Development of web interface for customer/seller login

In this module we would be developing a web interface for user login and signup. The module would use user name, password combination for login and signup. Here roles of the user would be defined based on seller and customer accounts.

While login we would be implementing a 3 step Kerberos authentication service as mentioned here, Network Security Application Level Authentication Kerberos. This would be our contribution to the paper that we are performing security in authentication as well, apart from the E-Commerce Module. In this authentication process customer/seller needs to first register himself/herself then he/she can make login to that particular web site. When user makes registration the password will be stored in database by encrypting it using sha1 algorithm.

- Development of Asymmetric Key Algorithm

An asymmetric key algorithm as mentioned in the paper would be developed to exchange data between the users. We would test this system initially with the help of text encryption and decryption. Asymmetric key algorithm is developed for receiving and transferring the data that means communication between customer/seller is not open. It

- Development of E-Commerce Module

For demonstration of security algorithm we would be developing a transaction module (funds transfer module), for a generalized E Commerce website. Once the customer purchases something from the seller, this module would help to transfer funds electronically from customer to seller. All the information regarding product purchase and fund transfer submitted to seller in encrypted format. Seller uses that information by doing decryption.

Integration of the E-Commerce Module with Asymmetric Key Algorithm

In this module, both modules 1, 2 and 3 would be combined in order to secure the transaction. This would demonstrate the use of Asymmetric Key Algorithm for providing security to the E-Commerce Transactions.

- Result evaluation and optimization

In this module results would be evaluated and optimization (if any) would be performed to get the optimal outputs.

**CONCLUSION**

Security is necessary in all aspects of fields. Kerberos provides third party authentication to prevent many different attacks occurred. The approach used in this paper attempts to prevent authentication attack by using three passwords, a new user must enter these passwords that will be stored on the Authentication Server. If an attacker gains access to TGT, then he can easily replay them to the TGS, but not to the Application Server (V). The reason for this is that attacker does not know the password to get session key used for communication with the Server V. So, we have to prevent attacks from taking unauthorized take control from system even if he has gain access to session key and the ticket. The approach used in our proposed architecture provides protection against replay and password attack.

**REFERENCES**

1. Ankur Chaudhary, khaleel ahmad, M.A. Rizvi, “E-Commerce Security Through Asymmetric Key Algorithm” published in IEEE computer society, 2014.

2. Niranjanamurthy, DR. Dharmendra Chahar, “Study of E-Commerce Security Issues and Solutions”, published in 2013.

3. Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar, “Database Security and Encryption: A Survey Study”, International Journal of Computer Applications June 2012.

4. Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, “Review of Attacks on Databases and Database Security Techniques”, International Journal of Emerging Technology and Advanced Engineering, November 2012.

5. Reyhaneh Tamimi, Prof. Dr. Mohammad Ebrahim Mohammadpourzarandi, “The Application of Web Usage Mining In E-commerce Security”, April 2013

6. Mark S. Ackerman, Donald T. Davis, “Privacy and Security Issues in E-Commerce”

7. Randy C. Marchany, Joseph G. Tront, “E-Commerce Security Issues”, 2002

8. Neetu Kawatra, Vijay Kumar, “Analysis of E-Commerce Security Protocols SSL and SET”, published in International Journal of Computer Applications 2011

9. William Stallings, Cryptography and network security principles and practices (4th ed., Pearson Prentice Hall, 2006).

10. Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.

11. Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management – IPCSIT vol.16 (2011)

12. Yang Jian, An Improved Scheme of Single Sign-on Protocol, Fifth International Conference on Information Assurance and Security, PP. 495-498, IEEE 2009.