Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Authentication Protocol in Client – Server Application using Visual Cryptography

Ms. Jasmin Bhambure, Ms. Dhanashri Chavan, Ms. Pallavi Band, Mrs.Lakshmi Madhuri

Department of Computer Engineering

Dr. D.Y.Patil School of Engineering, Lohegaon, Pune, India

Abstract- ***Kerberos is a network authentication protocol and 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 research, we used Kerberos Encryption Technique for authentication and transaction security in the network. Further, we created an Authentication Server that used to derive a Steganography image from user's password. This Steganography image was used for verifying user's identity and gain access for sever. The generated image then was used by authentication server, to encrypt ticket granting ticket + session key. The image generated by authentication server was then used by the Ticket granting server at the time of transaction through the transaction server to validate an authentic transaction. However, there was an issue of cross validation of the Stegonagraphic image by the transaction server for which we included to divide the image into two shares and distribute each to client and servers, while authentication the service server will combine both the shares and crosscheck with the ticket granting server which consist original image.***

Keywords—Decryption, Encryption ,password attack, Replay attack , steganography , Visual cryptography

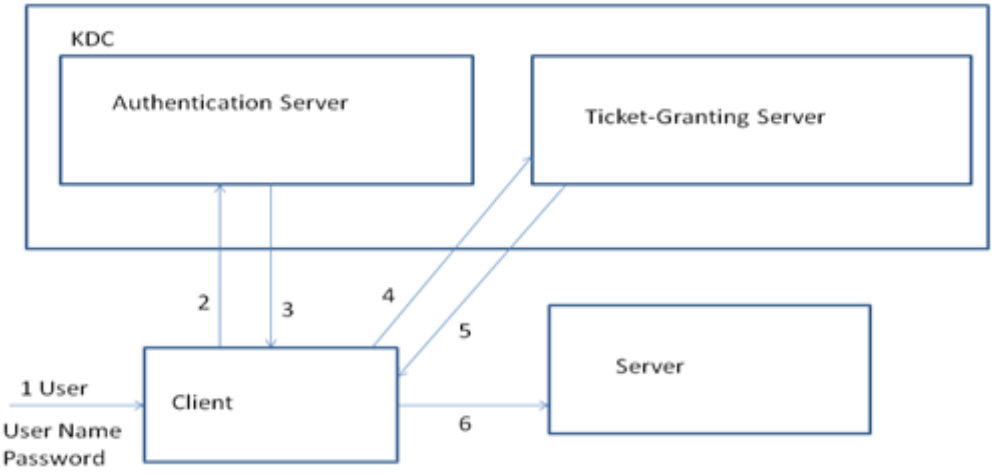
I. INTRODUCTION

Security in today's world is a major concern. As networks grow, they provide more and more services. Providing these services to the user in a secure way is an issue. Attackers can easily gain information during its transmission across the network and then gain unauthorized access to the servers, to whom they are not able to access.

WHAT IS KERBEROS?

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server. Two major problems with Kerberos **Replay attack** and **password attacks** are serious issues in the Kerberos authentication protocol. Many ideas have been proposed to prevent these attacks but they increase complexity of the total Kerberos environment. In this paper we present an improved method which prevents replay attacks and password attacks by using steganography and visual cryptography.

II. EXISTING SYSTEM OF KERBEROS

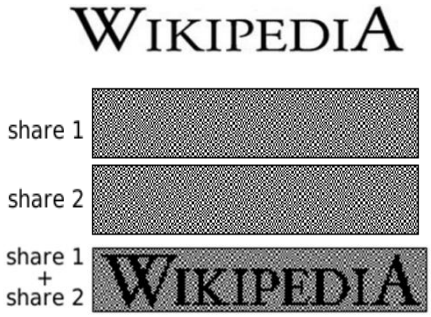


F ig.1 Existing Kerberos Architecture

1. Client's user name and password
2. Client providing the user name and password to authentication server
3. The authentication server generating ticket + session key gives to client
4. Client providing that ticket + session key to ticket granting server for granting ticket
5. Ticket granting server granting the ticket and sending it to client with timestamp
6. When all process is done in given timestamp then connection successful with client and server

III. VISUAL CRYPTOGRAPHY CONCEPT

Visual Cryptography (VC) is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares.



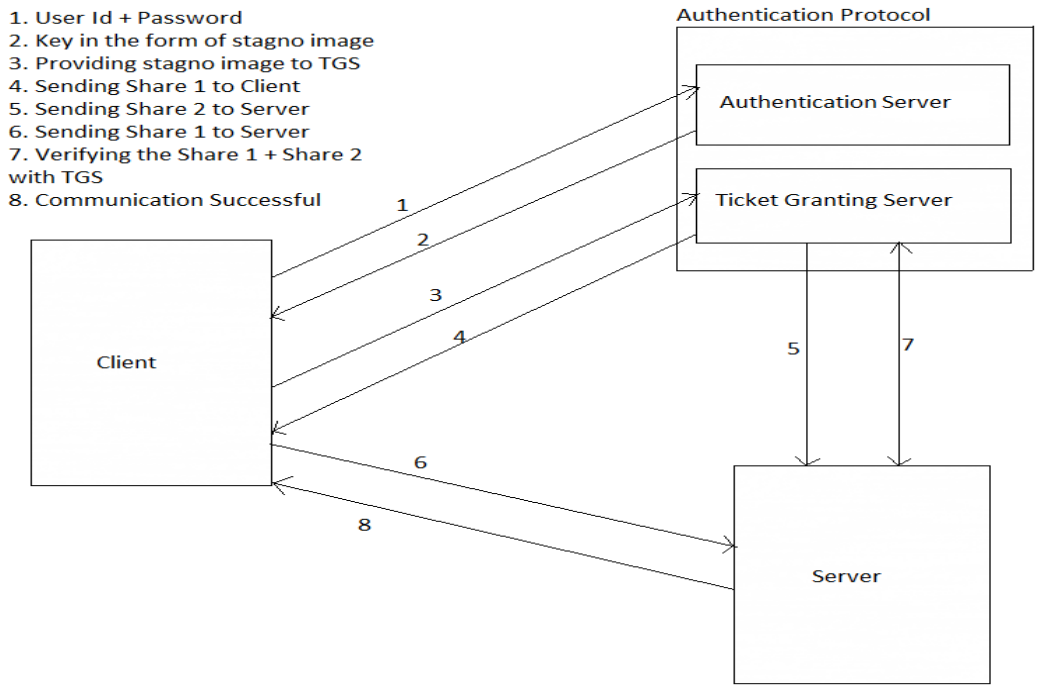
F ig.2 Visual Cryptography

IV. WHAT IS STAGNOGRAPHY?

STEGANOGRAPHY is a technique for information hiding. Steganography aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious. On the other side, steg analysis aims to expose the presence of hidden secret messages in those stego media. If there exists a steganalytic algorithm which can guess whether a given media is a cover or not with a higher probability than random guessing, the steganographic system is considered broken. In practice, two properties, undetectability and embedding capacity, should be carefully considered when designing a steganographic algorithm.

Usually, the larger payload embedded in a cover, the more detectable artifacts would be introduced into the stego. In many applications, the most important requirement for steganography is undetectability, which means that the stegos should be visually and statistically similar to the covers while keeping the embedding rate as high as possible. In this paper, it is consider digital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain.

V. PROPOSED SYSTEM



F ig.3 Proposed system of Kerberos

Main aims for this research to provide strong security to client-server application by creating steno image to provide services from server side. Authentication protocol consist of Authentication server and Ticket Granting Server. Authentication Protocol is provided with user information like registrations form , username or password, which encrypt the information in an stegoimage.Stegoimage is further provide to the client with a ticket to preserve one copy on client side. Client sends back Stegnoimage received from Authentication Server to Ticket Granting Server. Role of Ticket Granting Server is to make Share of this image i.e. Share1 and Share2.Share1 image is further provided to client and share2 is provided to server. Next, Client sends share1 to the server. Role of server is to combine Share1 and Share2 and cross-check with Ticket Granting Server. When both of the image match the server grants service to client.

VI. IMPLEMENTATION

MODULES

Module1 Steganoimage on client side

Module2 1.Authentication Server ,Steganoimage with session key

2.Ticket Granting Server , Steganoimage.Visual Cryptography

Module 3 Sever to provide services to client

Now to provide more security and authentication we have done encryption of the message using RSA algorithm. It is a Public key cryptography algorithm in which every user has two keys, one public key and one private key. The client will encrypt the text with the help of public key of the Server and the Server will decrypt the message by using its private key.Here we are talking about Authentication Server.

RSA ALGORITHM

1.1) pick two prime numbers, we'll pick p = 3 and q = 11

1.2) calculate n = p * q = 3 * 11 = 33

1.3) calculate z = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 20

1.4) choose a prime number k, such that k is co-prime to z, i.e, z I snot divisible by k. We have several choices for k: 7, 11, 13, 17, 19 (we cannot use 5, because 20 is divisible by 5). Let's pick k=7 (smaller k, "less math").

1.5) So, the numbers n = 33 and k = 7 become the Server's public key.

1.6) Now, still done in advance of any transmission, the Server has to calculate it's secret key. Here is how.

1.7) k * j = 1 (mod z) e.g 7 * j = 1 (mod 20)

1.9) (7 * j) / 20 = ? with the remainder of 1 (the "?" here means: "something, but don't wory about it"; we are only interested in the remainder). Since we selected (on purpose) to work with small numbers, we can easily conclude that 21 / 20 gives "something" with the remainder of 1. So, 7 * j = 21, and j = 3. This is our secret key. We MUST NOT give this key away.

Encrypting the message

2.1) P ^ k = E (mod n) "^" means "to the power of" P is the Plain message we want to encrypt n and k are Server's public key (see Section 1) E is our Encrypted message we want to generate After plugging in the values, this equation is solved as follows:

2.2) 14 ^ 7 = E (mod 33)

This equation in English says: raise 14 to the power of 7, divide this by 33, giving the remainder of E.

2.3) 105413504 / 33 = 3194348.606 (well, I lied when I said that this is "Pencil and Paper" method only. You might want to use a calculator here).

2.4) 3194348 * 33 = 10541348

2.5) E = 105413504 - 10541348 = 20

So, our Encrypted message is E=20. This is now the value that the Browser is going to send to the Server. When the Server receives this message, it then proceeds to Decrypt it, as follows.

Decrypting the Message

Here is the decryption math the Server executes to recover the original Plain text message which the Browser started with.

3.1) E ^ j = P (mod n)

E is the Encrypted message just received j is the Server's secret key P is the Plain message we are trying to recover n is Server's public key (well part of; remember that Server's public key was calculated in Section 1 as consisting of two numbers: n=33 and k=7).

After plugging in the values:

3.2) 20 ^ 3 = P (mod 33)

3.3) 8000 / 33 = ? with the remainder of P. So to calculate this remainder, we do:

3.4) 8000 / 33 = 242.424242...

3.5) 242 * 33 = 7986

3.6) P = 8000 - 7986 = 14, which is exactly the Plain text message that the Browser started with!

Replay attacks: Tickets can be copied or captured via sniffing and replayed at a later time. One attack involves copying a ticket, taking the client off the network (through a denial-of-service attack), impersonating the client's IP address, and resending the ticket. The authenticator was added to mitigate this attack. If the authenticator's timestamp is off by more than the clock skew (usually set to 5 minutes), the request is rejected. The security of Kerberos depends in large part on synchronized time, and therefore on the security of time synchronization protocols, which are often unauthenticated.

Spoofing such services is not trivial, but "it is not cryptographically difficult."To overcome this problem we have used Visual Cryptography concept.

Password-guessing attacks: The security of Kerberos depends on the secrecy of principal's keys. An attacker with a copy of Alice's encrypted credentials (sniffed or copied from the local system) can attempt to discover Alice's password by guessing or brute-forcing keys to decrypt the session key. Kerberos allowed unauthenticated requests for any client's encrypted credentials, meaning an attacker could simply request a victim's encrypted credentials. Kerberos 5 introduced the Pre-Authentication option to mitigate this attack, in which the client in also encrypts the current time with its secret key. The KDC then decrypts the time with the client's key and verifies it before sending credentials. Password-guessing attacks are still possible if an attacker obtains credentials through other methods.

Visual CryptoGraphy Algorithm: X-OR Visual cryptography is a cryptographic technique which allows image to be encrypted in such a way that after decryption we get the original image which was not possible with normal visual cryptography. The decoding is done by the human visual system directly or with the help of computer.

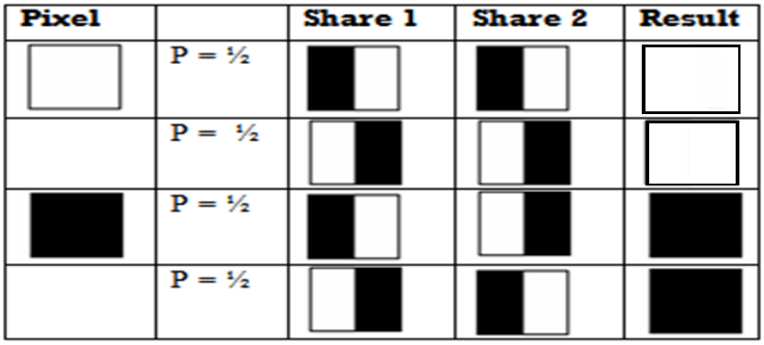


Fig 4: 2 out of 2 Scheme (2 subpixels)

VII. RELATED WORK

Two major problems with Kerberos **Replay attack** and **password attacks** are serious issues in the Kerberos authentication protocol. This research is based on improved Kerberos architecture by using visual cryptography and steganoimage. Main aims for this research to provide strong security to client-server application by creating steno image to provide services from server side. When client providing the user name and password to the authentication server it will encrypting for removing password attack.

Authentication protocol consist of Authentication server and Ticket Granting Server. Authentication Protocol is provided with user information like registrations form , username or password, which encrypt the information in an stegoimage.Stegoimage is further provide to the client with a ticket to preserve one copy on client side.

Client sends back Stegnoimage received from Authentication Server to Ticket Granting Server. Role of Ticket Granting Server is to make Share of this image i.e. Share1 and Share2.Share1 image is further provided to client and share2 is provided to server. Next, Client sends share1 to the server. Role of server is to combine Share1 and Share2 and cross-check with Ticket Granting Server. When both of the image match the server grants service to client.

VIII. CONCLUSION

Security is always an important issue whenever a transaction is carried in network. We usually need to share the data with authorized client only. For ensuring authentication of the clients there are several protocols available and Kerberos is one of them. In this project we have made an attempt to enhance the security issue by using the concept of Kerberos. We have implemented the highly authenticated transaction scheme in which Authentication server creates a ticket which is further encrypted using the secret key shared by the server and authentication Server. This ticket is then sent back to client.

REFERENCES

1. Eman El- Emam, Magdy Koutb, Hamdy Kelash, and Osama Farag Allah, "An Authentication Protocol Based on Kerberos5", *International Journal of Network Security, Vol.12, No.3, PP.159{170, May 2011.*
2. Vijendrasinh Thakur , K. N. Hande "Improving Kerberos Security Using Dynamic Password Based Authentication" *International Journal of Emerging trends in Engineering and Development Issue 2, Vol.7 (November 2012)*
3. Priyanka Rajesh Gulhane and Prof. V. T. Gaikwad " Kerberos The Network Authentication Protocol", *International Journal of Computer Information Systems, Vol. 2, No. 3, 2011*
4. Vinod Shokeen , Niranjan Yadav "Encryption and Decryption Technique for Message Communication" *International Journal of Electronics & Communication Technology Vol. 2, Issue 2, June 2011*
5. E. Thambiraja ,G. Ramesh "A Survey on Various Most Common Encryption Techniques" *International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012*
6. Gagan Dua1, Nitin Gautam2, Dharmendar Sharma3, Ankit Arora4 , "Reply Attack Prevention In Kerberos Authentication Protocol Using Triple Password*" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013*

7. David William McBride "Building a Better Grid Authentication System with Kerberos" *University of London Imperial College of Science, Technology and Medicine Department of Computing May 2011*
8. Stuart J Rogers, SAS Institute Inc., Cary, NC " Kerberos and SAS® 9.4: A Three-Headed Solution for Authentication" *SAS Global Forum 2013*
9. *William Stallings*, Cryptography and network security principles and practices *(4th ed., Pearson Prentice Hall, 2006).*
10. V.K. Pachghare , Cryptography and information security*(Estern Economy Edition 2009)*

