International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 11218-11223

A Modified Approach for Kerberos Authentication Protocol with Secret Image by using Visual Cryptography

Ashok Kumar J[1], and Gopinath Ganapathy[2]

[1,2]School of Computer Science, Engineering and Applications Bharathidasan University, Tiruchirapalli, Tamil Nadu 620023, India.

[1]Orcid Id: 0000-0002-4969-8257

Abstract

Kerberos is an authentication protocol in which client and server can mutually authenticate to each other across an insecure network connection, to ensure data integrity of the message and privacy of channel communications. In this paper, a new novel is proposed to improve Kerberos authentication protocol by using Secret Image. This proposed modification in Kerberos will be modified to yield better security solutions and to provide centralized access control policy for each user with different parameters like authentication, speed of encryption and decryption and efficiency of transactions. This modified approach enhances the secure authentication of users with non-reputation feature by incorporating public key cryptography and hiding the message of differential access control for each user by using secret image. This differential access control policy is being enforced directly to the clients while doing the authentication of users through Kerberos protocol. The GnuPG has the capability to generate the key pair (ie, private key and public key) in the client itself. So this proposed system used this key pair for encryption and decryption of messages and takes the advantage of non transferring or non importing the private key from any devices or any nodes.

Keywords: Kerberos, Visual Cryptography, GnuPG

INTRODUCTION

In a client-server architecture, the server is responsible to provide the service to client in an organized manner and client utilizes those services to perform the desired task which is assigned specifically for the user. In an unprotected network environment, an opponent client can make request to any server for service to obtain the unauthorized privileges in a server machine as obvious security risk is that of impersonation. In order to overcome the impersonation risk, the server has to maintain an identification of each client to authenticate those clients by providing the credentials of that user. In an open environment, the substantial burden is placed on each server. An advantage of using client-server is the ability to connect remote users with remote resources to conform the authorization and authentication aspect of secure distributed system. Authorization specifies the access rights for the user to access the specific resource to identify the nodes by authenticating the user to maintain high degree of confidence[1].

Kerberos is a protocol widely used for the authentication mechanism for the client-server environment. Kerberos contains three main parts such as, key distribution centre (KDC), AS (Authentication service), and TGS (Ticket granting service). Kerberos is working with two types of ticket and they are called as Ticket Granting Ticket (TGT) and Service ticket (SGT). TGT is used to validate its ticket at KDC, whereas Service ticket is to be validated at Application Server. Once the Kerberos grants the ticket, the user does not need to login again every time to communicate with KDC and they will get service tickets for accessing different Application Servers [2]. The ticket TGT is transmitted from client to server and then it is verified for each successful decryption of packet. This process always be a burden to server and it utilize more computation power to balance the load of the server. The attacker can send any message to Authentication server which is always ready to provide the ticket without verifying the incoming request and so the attacker can guess a password with the obtained ticket. Kerberos does not provide the authorization policy for the user after they successfully authenticated in the client system.

Visual Cryptography (VC) was first proposed by Moni Naor and Adi Shamir in 1994, used to encrypt secret images in such a way that it can be decrypted by the human visual system. These encryption techniques do not need any cryptographic computation [3]. Visual Cryptography is a technique of encrypting a secret image into number of shares such that stacking a sufficient shares of secret image reveals the original image with simple computation for decrypting. The shares of Visual Cryptography in sequence can be transmitted to any network and can be obtained the original (secret) image by stacking them. A hacker could predict the secret information only it is possible to collect all the shares that are passing in the sequence over the network. To overcome this issue, the secret shares of Visual Cryptography are to be secured by using Public Key Cryptography. Thus the hackers are prohibited from retrieving the original (secret) image without having the private key [4].

This paper explains about the existing authentication mechanism and provides the security analysis for Kerberos V protocol and then proposed the new approach for improving Kerberos protocol with Secret Image by using Visual Cryptography. Finally, it analysis the proposed security scheme in a client server network.

KERBEROS V EXISTING AUTHENTICATION

Kerberos protocol works based on the ticket based system in which Key Distribution Center (KDC) issues ticket encrypted with user's password and user decrypts it to obtain tickets for accessing the requested server or services [2] [5].

The three components of Kerberos protocol are (see Fig. 1):

1) Client: It is the user available in the client system to request the service from any servers in the distributed system.

2) Key Distribution Center: KDC holds all the information about users and secret key for the requested service to authenticate the user. It has two components and they are Authentication Server (AS) and Ticket Granting Server (TGS). The AS authenticates the user by verifying the user and TGS is responsible to issue a ticket for the user to obtain the service from the application server.

3) Application Server: The application server provides specific services for the user.

KERBEROS AUTHENTICATION PROCESS

Kerberos is an authentication mechanism for authenticating the client to the server in the client-server environment. It is assumed that the user's password is shared securely to the client. When logging, the user suppose has to provide username and password, then the client will request service with AS, secret key is then generated by using client's password at AS. Kerberos acts as a trusted third party in between the server and client to authenticate mutually. The AS contains the username and passwords in its KDC database. Table 1 and Table 2 show the abbreviations used to describe the protocol. The following six steps brief the client authentication messages with application server(See Table 1 for Message No and its message information):

Step 1: Client sends both user's ID and ID of TGS to AS with a request of TGT.

Step 2: AS encrypts the ticket with client's password and sends to client. The client will then decrypt the ticket by using correct password.

Step 3: Client sends the TGT , service ID and user's ID to TGS with a request of Service Granting Ticket (SGT).

Step 4: TGS decrypts incoming ticket and verifies with the presence of its ID and expiry of the lifetime. It issues a SGT to the client for accessing the server V, if incoming information has valid user ID and network address.

Step 5: Client receive the SGT from TGS. Then it sends this ticket SGT along with user ID to the server for accessing a service. The server verify the ticket and authenticate the user.

Step 6: Server V opens the communication with client C. Then it uses the key Kc,v to encrypt the received timestamp by adding 1 in to that message. Then it sends this encrypted message to the client to verify the identity of V in client system.

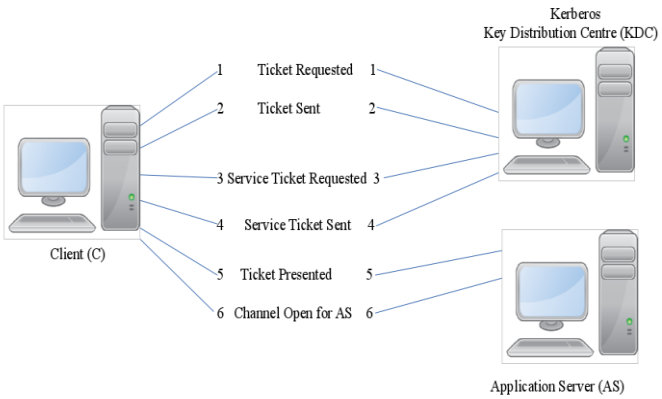

Figure 1: Traditional Kerberos Authentication Protocol

Table. 1. Traditional Kerberos Authentication Protocol

Message No.	Message Exchange
1	$C \rightarrow AS: ID_C \| ID_{tgs} \| TS_1$
2	$AS \rightarrow C : E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$ $Ticket_{tgs} = E(K_{tgs}, [K_{c,v} \| IDC \| ADC \| IDv \| SN4 \| Lifetime4])$
3	$C \rightarrow TGS : ID_v \| Ticket_{tgs} \| Authenticator_c$ $Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$
4	$TGS \rightarrow C: E(K_{c,tgs},[K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$ $Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$
5	$C \rightarrow V : Ticket_v \| Authenticator_c$
6	$V \rightarrow C : E(K_{c,v}, [TS_5 + 1])$

Table. 2. Abbrevations used in Kerberos Authentication Protocol

Symbol	Meaning
C	Client
V	Server
TGS	Ticket Granting Server
AS	Authentication Server
ID_c	Identifier of user on C
ID_v	Identifier of V
K_X	Secret key for X
$K_{X,Y}$	Session key between X and Y
Lifetime	Ticket's Validity
AD_c	Network Address of C
TS	Time stamp of data packet
$Authenticator_X$	Authenticator for X
$Ticket_X$	X's authorization ticket
$\|$	Concatenation

KERBEROS SECURITY ANALYSIS

Kerberos is a secure, trusted third party protocol for authentication in a distributed network environment. There are some weaknesses in Kerberos due to the limitation in design and some drawbacks [5].

Kerberos has following limitations:

a) Password Guessing Attack: It is possible for the attacker to send any message to the Authentication Server and could receive the ticket from Kerberos as authentication is not required. It leads to guess the password and request many tickets by the attacker.

b) Access Authorization : Authentication verifies the user identity and authentication enables authorization. But Kerberos does not provide the authorization access for the user in the client.

c) Replay Attack: Kerberos uses the timestamp mechanism to avoid the unauthorized authentication as the attacker can replay the same messages again and again. If the attacker can replay the message within stipulated time of the user authentication, then this timestamp mehanism is useless.

d) Dictionary Attack: The user's password is used as secret key to encrypt the message from AS to Client. If the key is not strong, then there is a possibility for dictionary attack.

e) Key Storage Problem: The key management and maintenance of symmetric key in KDC will be the biggest problem in Kerberos protocol.

f) Malware Attack: It is possible for the attackers to design the client softwares to suit with kerberos protocol for installing the malware in the client systems. Then this malware will redirect all the users operations including password inputting to invade KDC, and disguise as KDC to complete the man in the middle attack

g) Authentication Forward Problem: Kerberos 5 has a new feature added called authentication forwarding. It means when a client is granted access to a server, it can let this server act as a client to apply for a different server. This leads to springboard attack.

h) Unauthorized Database Access: The compromised database of the Kerberos KDC can easily be attacked to get the credentials such as username and passwords of all the clients.

i) Single Point of Failure: The client has to send request continuously for the availability of Kerberos Server, otherwise the application service for each client will be lost.

j) Clock Synchronization: The authentication of each client system depends upon the synchronization of Kerberos Server clock.

k) Digital Signature: Kerberos does not have undeniable mechanism because it cannot fulfill the purpose of digital signature.

Improvement of Kerberos Authentication based on Secret Image

After this extensive study on traditional Kerberos protocol, it is noticed that the security issues mentioned in the section “Kerberos Security Analysis” can be modified to yield better security solutions on different parameters like authentication, speed of encryption and decryption and efficiency etc. The modified proposed approach had enhanced the secure authentication of users with non-reputation feature and with differential access control for the user. The Kerberos authentication is replaced with the Visual Cryptography technique for securely authenticating the users by improving the efficiency of the Kerberos system. The differential access control mechanism for each user is being enforced directly in to the clients while doing the authentication of client with Kerberos protocol. The proposed idea not only solves the problem mentioned in the section “Kerberos Security Analysis”, but it improves overall performance, enhanced the security with the use of secret image based authentication and providing differential access control policy for each user and efficiency of Kerberos protocol.

Idea behind this proposed approach

Compare to Asymmetric algorithms, Symmetric algorithms are fast and provides confidentiality. But Asymmetric algorithms has no drawbacks like Symmetric algorithms such as difficult key management and lack of scalability. Each type of algorithm has its own merits and demerits, so using them together can be the best of both worlds. Mazhar Islam et al. proposed a new symmetric key encryption scheme with “Image as Secret key” and has the advantage of very large key size. It provides the comparison value based on throughput of packet size with various symmetric keys algorithm and they are AES as 5.3 , 3DES as 4.5, DES as 5.2 and the Image as Secret key as 136.06 [6]. But the author Siddaram Shetty et al. proposed the new technique of securing image-based secrets by encrypting the generated image shares of Visual Cryptography using Public key Encryption. In the scheme of Visual cryptography, decryption of the secret images can be done without the need of cryptography computations. The author explains “it is more secure and very easy to implement with low computation cost. The original image is divided into shares after converting it into binary image, next the shares of binary image are encrypted and decrypted by using RSA algorithm, because of this, even if the unauthorized person,

once getting all the shares, they can't get back the original secret image without availability of the private key" [4]. In this proposed scheme, the client private key is available in the client system itself and it can not be transferred with any medium, So the only responsibility of the client is to decrypt the image. It is more secure approach and the secret image can hold the enough data for access control information about the authenticating user.

In traditional Kerberos authentication, using passwords as symmetric key is easily broken by the hackers. So the authentication method has to be replaced with public key instead of using symmetric key. GnuPG is based on the concept of "web of trust model" to establish the authenticity of the binding between a public key and its owner [7]. It does not require centralized certification authorities, but instead rely on trust relationships between regular users. The proposed scheme combines the advantages of both Visual Cryptography as well as GnuPG Public Key Cryptography. This scheme enhances the security of VC shares by encrypting with OTP and then with Public Key Cryptography, which provides the strong security for secret images to transfer the information within secret images. "Modified Client Authentication Responsibility in Kerberos Protocol" study revealed about new process model that aims the responsibility of the client to authenticate itself instead of the server is doing this task [8]. This reduces the burden on the server and make the server is constantly available. In this proposed scheme, Authorization token (TGT) is removed from the traditional Kerberos Authentication and will replace the client based authentication with the use of visual cryptography. Hence this methodology reduced server burden and clients are getting authenticate itself with the server and will get the access privileges to access the application server in order to enhance its security and reduce the unauthorized server interactions.

The most dominant problem for the distributed systems to compute the data in the node is access control mechanism for ensuring data security and privacy of the data in that node. The author focuses his approach with access control mechanism to act as a trusted third party between distributed system servers and clients to allow securely access the services with differential user access control privileges [9]. In the proposed scheme, after authenticating the user in the KDC, the access control policy for the user will be embedded with the secret image and enforced into the client system through the concept of "Secure Visual Cryptography Scheme for Sharing Secret Image using RSA".

Proposed Design scheme for Kerberos protocol with Secret Image

In the proposed scheme, the traditional Kerberos message exchange steps step 1, step 2 , step 3 and step 4 (Fig. 2) will be modified based on the concept of visual cryptography. It is assumed that each client generated the GnuPG public key and private key by itself in the secure manner and stored securely in the client system itself. Then this GnuPG public key must be registered securely with the KDC database and the same way TGS server should share the one part of "shared image A" with the user to authenticate themself each time the user want to login into the Kerberos server. But the other part of the "shared image A" will be kept in TGS server and not to be disclosed with any node or any user. Thus the user authentication for server is based on secret image "shared image A" which is available in the client and for the client, authentication is based on the another Secret image "shared image B". Secret image "shared image B" contains the access control mechanism for the specific user and it will be splited into the two images based on the concept of Visual Cryptography. It is then encrypted with the OTP which is based on the cipher text used in the methodology "Image as Secret key" and then OTP is encrypted with client public key to provide access control policy for that user. Then the client decrypt the first share image "shared image B" and wait for the second share image "shared image B" from the server. If both the share image is available in the client system, then the private key is used to decrypt the OTP and OTP is used to decrypt both shared images. If the two shares are matched based on the visual cryptography technique, then the authentication is successful otherwise the client process will be discarded. After the successful authentication, the original image is retrieved and so that the access control policy will be enforced for the authenticated user. The timestamp mechanism of traditional Kerberos protocol is replaced with the sequence number mechanism.

The improved Kerberos protocol is as follows (see Table. 3 and Table. 4).

Step 1: Client sends the user ID, its secret share one "shared image A" and sequence number (SN) to the AS.

Step 2: At KDC, the AS receives the secret share of first part "shared image A" from the client. Then it stacks this first secret share with already available second part "shared image A" in the database. It will generate a new computed image with these two secret shares and it will be verified with original image. If it is success, then AS generates the another secret image "shared image B" and splits the secret image as two by using the concept of visual cryptography. This secret image "shared image B" contains the access control information for the authenticating user. Then this one part of secret image "shared image B" is encrypted with session key One TimePassword (OTP) and then this OTP will be encrypted with public key of client. Then AS sends it to the client.

Step 3: The client decrypts the OTP with private key and then using this OTP it decrypts the secret image "shared image B". Then it transmits the Authenticator and secret share "shared image A" to the TGS. Still the client needs second secret image "shared image B" to authenticate itself and enforce the access control policy for the user.

Step 4: At KDC, the AS stacks the secret share one "shared image A" which came from the client as explained in the stage 2, then AS encrypts the another part 2 secret image "shared image B" and sends it to the client which contains the secret session key which is used to provide secure communication between client and server.

Step 5: Then the client sends the ticket to the application server which is granted from KDC.

Step 6: The client gets the acknowledgment from the application server after successful verification of client.

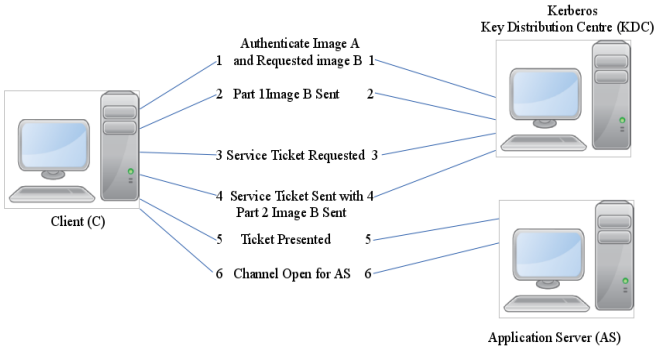

Figure 2: Improved Kerberos Authentication Protocol

Table. 3. Improved Kerberos Authentication Protocol

Message No.	Message Exchange
1	$C \rightarrow AS: ID_C \| ShareA\_1 \| SN_1$
2	$AS \rightarrow C : E(OTP, [K_{c,tgs} \| ID_{tgs} \| SN_2 \| Lifetime_2 \| ShareB\_1]) \| E(PU_C, OTP)$
3	$C \rightarrow TGS : ID_v \| ID_{tgs} \| ShareA\_1 \| Authenticator_c$ $Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| SN_3])$
4	$TGS \rightarrow C: E(K_{c,tgs}, [K_{c,v} \| ID_v \| SN_4 \| ShareB\_2 \| Ticket_v])$ $Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| SN_4 \| Lifetime_4])$
5	$C \rightarrow V : Ticket_v \| Authenticator_c$
6	$V \rightarrow C : E(K_{c,v}, [SN_5 + 1])$

Table. 4. Abbrevation used in Improved Kerberos Authentication Protocol

Symbol	Meaning
C	Client
V	Server
TGS	Ticket Granting Server
PR_x	Private key for x
PU_x	Public key for x
ID_x	Identifier of user on x
$K_{X,Y}$	Session key between X and Y
Lifetime	Ticket's Validity
SN	Serial Number for Packet
Image_i_share_j	i is the image number for A & B. j is the share no of the image i from 1 to 2.
||	Concatenation
E	Encryption
OTP	One Time Password
AS	Authentication Server
AD_c	Network Address of C
TS	Time stamp of data packet
$Authenticator_X$	Authenticator for X
$Ticket_X$	X's authorization ticket

ANALYSIS OF PROPOSED SCHEME

Feasibility Analysis

The improved scheme modified the authentication structure with the use of Visual cryptography as a post-authentication in the client system, it works as an extra layer of security in Kerberos and enforcing the access control mechanism of that authenticated user through secret image. Secret image has the advantage of stacking a sufficient shares of secret image reveals the original image with simple computation for decrypting and it does not involve any cryptography computations. The GnuPG generates the key pair (ie, private key and public key) in the client itself and takes the advantage of non transferring or non importing the private key from any devices or any nodes. It establishes trust relationships between regular users and the public key/private key in the client system.

BENEFITS OF PROPOSED METHOD

1. The Visual Cryptography is used as a pre-authentication for AS and TGS and so the user authentication is based on secret image "shared image A". It does not need any cryptography computations for decryption and encryption. So it is highly secured for authenticating the user.
2. The authentication and authorization access for client is based on the another Secret image "shared image B". Secret image "shared image B" contains the access control mechanism for the specific user and it will be splited into the two image based on the concept of Visual Cryptography. After the successful authentication, the original image is retrieved and so that the access control mechanism will be enforced for the authenticated user.
3. Each client generated the GnuPG public key and private key by itself in the secure manner is stored securely in the client system itself. The problems of key distribution with symmetric key management are solved by using public key algorithm.
4. The timestamp mechanism of traditional Kerberos protocol is replaced with the sequence number mechanism. This prevents from the replay attack.
5. Password guessing attack is not possible because one time password (OTP) is used, instead of the client password.
6. The client private key is available in the client system itself and so the only responsibility of client to decrypt the secret shared image. It is more secure than the traditional authentication and secret image can hold enough data for access control information about the authenticating user to enforce it into the client system directly.

7. The proposed scheme uses public key encryption and thus guarantees Digital Signature mechanism.
8. This approach resolves the problem in distributed systems for computation of data in the node by enforcing access control mechanism within Kerberos protocol itself for ensuring data security and privacy of the data in that node.

CONCLUSION

In this paper, a novel approach is proposed by incorporating Visual cryptography and GnuPG Public key Cryptography into Kerberos protocol. The Visual cryptography is used for enforcing the access control mechanism to authenticated user through secret image. To securely exchange the secret image between the client and KDC, the GnuPG public key is used to encrypt and decrypt it. The original image in the KDC is divided into shares after converting it into binary image, next the shares of binary image are encrypted and decrypted by using ECC algorithm, because of this even if the unauthorized person, once getting all the shares, they can't get back the original secret image without availability of the private key. Moreover the client private key is available in the client system itself and so the only responsibility of client to decrypt the image. It is more secure than the traditional authentication and secret image can hold enough data for access control information about the authenticating user to enforce it into the client system directly. It is considered that this work is a novel step towards further improvement of Kerberos authentication protocol.

FUTURE WORK

The traditional Kerberos protocol does not imply the access control policy for the user in the protocol itself. In this novel approach, it is proposed to integrate the access control policy through the concept of visual cryptography and the use of secret image to embed the access control policy information for the Kerberos authorization services to be enable in the client systems. This feature of access control policy for the user will be analyzed separately in future to enforce the various access control techniques with different set of policies for user in the client system.

REFERENCES

[1] Aruna kumari, Shakti mishra & Kushwaha. (2010). A New Collaborative Trust Enhanced Security Model for Distributed System. *International Journal of Computer Applications*, 1(26), 117-123.

[2] William stallings (2006). *Cryptography and network security principles and practices*. (4th ed ed.). Pearson Prentice Hall.

[3] moni naor & adi shamir. (2017). *Visual Cryptography*. Retrieved 22 September, 2017, from http://www.fe.infn.it/u/filimanto/scienza/webkrypto/visualdecryption.pdf

[4] Siddaram shetty & minu p abraham. (2015). A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA. *International Journal of Innovative Research in Computer and Communication Engineering*, 3(4), 3331-3336.

[5] Naman S. Khandelwal and Pariza Kamboj (2015) ,"Two Factor Authentication Using Visual Cryptography and Digital Envelope in Kerberos," Published in: Electrical, Electronics, Signals, Communication and Optimization (EESCO), International Conference

[6] Mazhar Islam, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Muhammad Jamil Khan (2015). "A New Symmetric Key Encryption Algorithm using Images as Secret Keys" , 13th International Conference on Frontiers of Information Technology

[7] Michael louie loria. (2014). *Pretty Good Privacy*. Retrieved 21 August, 2017, from http://slidedeck.io/michaellouieloria/pgp

[8] Ali m meligy, Walid a dabour & Alaa s farhat. (2013). Modified Client Authentication Responsibility in Kerberos Protocol. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(12), 357-362.

[9] Santosh khamitkar et al.. (2015). Kerberos Authentication With Cloud Computing Access Control. *International Journal of Advanced Computational Engineering and Networking*, 3(6), 36-41.