International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Modified Authentication Protocol and Evaluation Tool: Kerberos and BAN Logic

Randhir Bhandari, Digvijay Puri, Natasha Sharma

Abstract: ***In today's world the computer network communication increases the efficiency most of the organizations. Hence threats have been increased due to these online transactions/communications. These threats necessitate the researchers to improve the existing security protocols and /or develop the new ones. Authentication Protocols are one of the same which can provide the authentication, confidentiality & integrity. For checking the authenticity of messages exchange process in authentication protocols BAN logic is used. The Kerberos encrypt the information for authentications. Many organizations use it and it has five versions and versions 4 and 5 are latest. In one of over previous paper we have generalized the ticket exchange process of version 5. In this paper to make it more authenticated some modifications are proposed to both BAN and Kerberos and we defined them as R- Kerberos & R-BAN. To achieve this, we have added participant's physical address (MAC Address) as it is unique to every network adapter and can be used as our secret key.***

Index Terms—NTLM, Kerberos, BAN, cryptography, encryption, decryption, ticket.

I. INTRODUCTION

In beginning of computer era, the security of data mostly depends on the user or system and the authenticity of the user depend on the single password set by the user only. When the Windows based environment started the passwords were stored on the client machines only. To enhance the authentication measures, Microsoft introduced LAN Manager or LM [8] as an authentication protocol. The LM was used in Windows 95, NT 3.5 and earlier versions. The LM password length was restricted to 14 characters only and every seven characters are encrypted separately [8]. The LM could not distinguish between the upper- and lower-case characters. Later to overcome these limitations LM was enhanced and the new protocol NTLM which came into existence in 1993[7] and was a challenge – response type protocol. This protocol was used on different networks that included Windows operating systems. Also, this protocol can operate on stand-alone systems. In the beginning for authentication Microsoft used NTLM protocol in windows NT and is still incorporated with new versions (Windows 7,8) for the compatibility with older versions (Win9X,NT4.0,SP4)[7].

Manuscript published on 30 September 2019
* Correspondence Author
Randhir Bhandari*, Senior Faculty-IT, iNurture Education Solutions Private Limited, Banglore, India. Email: jobrandhir@gmail.com
Digvijay Puri, Senior Faculty-IT, iNurture Education Solutions Private Limited, Banglore, India. Email: digvijaypuri@gmail.com
Natasha Sharma, Faculty-IT, iNurture Education Solutions Private Limited, Banglore, India. Email: natasha.sharma1003@gmail.com

Retrieval Number C4684098319/2019©BEIESP
DOI: 10.35940/ijrte.C4684.098319
Journal Website: www.ijrte.org

Microsoft does not recommend NTLM as the recent cryptographic techniques like AES or SHA 256 are not supported in this protocol. NTLM works on Cyclic Redundancy Check (CRC) or Message digest algorithm to provide integrity of data and it incorporates RC4 cryptographic method for encryption. NTLM comes with Version 1 and 2.

NTLM v1 sends 8-byte random number and secret key (password) to communicate with server, but as it is prone to a dictionary attack so NTLM v2 came in existence. It includes MD4 hashed 8-byte client.According to Greek's Kerberos is a three headed dog which guard the house of Hades. The authentications, accounting and authorization represents three heads of the dog.

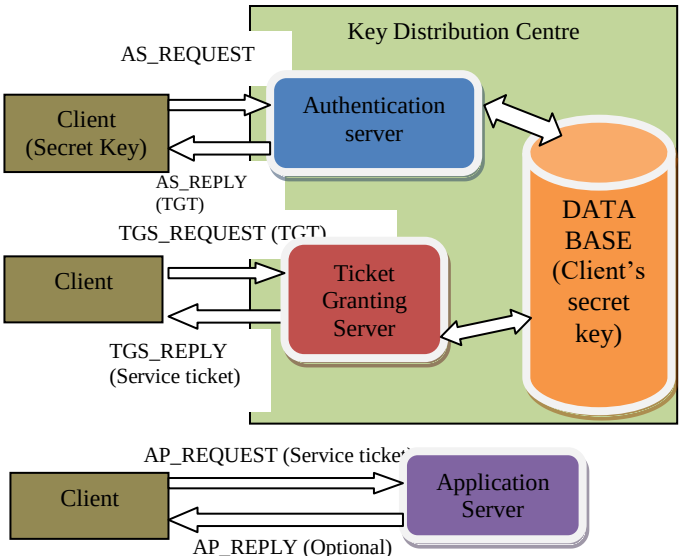

Fig. 1: Ticketing process in Kerberos [4]

The Kerberos is basically providing authentications and hence is called authentication protocol. Kerberos is developed by MIT[5] which secures the networks by using methodology of private key encryption. For authentications third party is responsible in Ker brose and is called as authentication servers. We have 5 versions of Kerberos but version 4 and version 5 are only used for administrations environments.

The BAN logic developed by M. Burrows, M. Abadi and R. Needham in 1990. The BAN logic tries to verify the authentication protocols by achieving some goals that user had in mind and are the basic goals that must be satisfied for achieving the authenticity of the protocol.

II. FUNCTIONING OF KERBEROS

C ⟶ KDC (AS_REQUEST): Key Distribution center (KDC) contains authentication server to whom the client provides its identifications by presenting its credentials.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

KDC ⟶ Client (AS_REPLY): When authentication server gets request from the client for authentication it provides Ticket Granting Ticket and session key to the client.

C ⟶ KDC (TGS_REQUEST): In this step Ticket Granting Server gets requests from client for getting service ticket.

KDC ⟶ Client (TGS_REPLY): As TGS get request fir service ticket in response, it provides service ticket to the client.

C ⟶ AP (AP_REQUEST): the service ticket obtained from Ticket Granting Server is presented to application server

AP ⟶ C (AP_REPLY): In this application server proves it's authenticity to the client.

III. PHASE-1 TICKET GENERATION

Ticket Granting Ticket

1. $C \rightarrow KDC: U, Service, nu$
2. $KDC \rightarrow \{T_{c,s}\}K_s : \{C, lt, K_{c,s}\}K_s$
3. $KDC \rightarrow Client: \{K_{c,s}, n\}K_c, \{T_{c,s}\}K_s$
4. $(A_c) = \{C, ts\}K_{c,s}$
5. $C \rightarrow Server: \{A_c\}K_{c,s}, \{T_{c,s}\}K_s$

(In version 4, message 3 is $\{k_{c,s}, n, \{T_{c,s}\}K_s\}K_c$ }) [2]

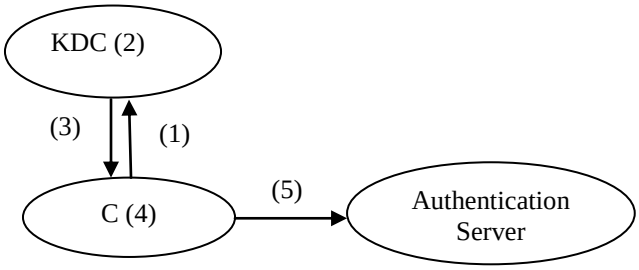

Fig. 2: TGT creation Process [4]

IV. TICKET GRANTING PROCESS

Ticket Processing

(1) In first step the client provides its information to authentication server for getting authenticated. It presents name of the client, service and a non-repeating identifier.

$$C \rightarrow KDC: U, Service, n$$

(2) In this random encrypted key is generated i.e. ($K_{c,s}$).

$$KDC \rightarrow \{T_{c,s}\}K_s : \{C, lt, K_{c,s}\}K_s$$

(3) In this step a shared secrete key is used for encrypting lifetime and session key of TGT.

$$KDC \rightarrow C: \{K_{c,s}, n\}K_c, \{T_{c,s}\}K_s$$

(4) A authenticator (A_c) is generated by client and gets it encrypted using ($K_{c,s}$) which holds (ts) and user (U).

$$(A_c) = \{C, ts\}K_{c,s}$$

(5) In this step the information of client and session key is decrypted.

$$C \rightarrow Server: \{A_c\}K_{c,s}, \{T_{c,s}\}K_s$$

(6) In this step authenticator is decrypted by authentication server for verifying the time stamp.

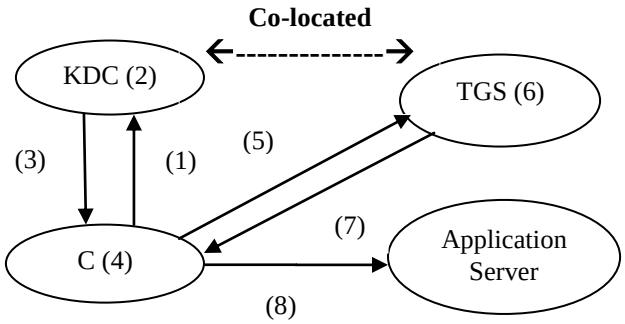

Fig. 3: Ticketing Process for TGS [4]

TGS

1. $C \rightarrow TGS: U, tgs, nu$
2. $TGT = T_{c,tgs} = U, Service, nu, lt, K_{c,tgs}$
3. $TGS \rightarrow C: \{K_{c,tgs}, n\}K_c, \{T_{c,tgs}\}K_{tgs}$
4. $A_c = \{U, ts\}K_{c,tgs}$
5. $C \rightarrow TGS: A_c, \{T_{c,tgs}\}K_{tgs}, S, nu$
6. $T_{c,s} = T_{service} = U, Service, nu, IPlist, lt, K_{c,s}$
7. $TGS \rightarrow C: \{K_{c,s}, nu\}K_{c,tgs}, \{T_{c,s}\}K_s$
8. $C \rightarrow Server: \{A_c\}K_{c,s}, \{T_{c,s}\}K_s$

(In version 4, message 3 is$K_{c,tgs}, nu, \{T_{c,tgs}\}K_{tgs}\}K_c$, and message 5 is $\{K_{c,s}, nu, \{T_{c,s}\}K_s\}K_{c,tgs}$) [2]

V. PHASE-2 TGS

In first phase of ticket exchange clients started the communication with server for getting service ticket in this process client communicates with TGS which is part of KDC and helps in making environment transparent.

Step 1: In first step client provides its information like name(U) timestamp (nu) to the TGS.

$$C \rightarrow TGS: U, tgs, nu$$

Step 2: In the equation-2 TGT is further simplified and contains username (U) service name(service) lifetime(lt) and session key ($K_{c,tgs}$).

$$TGT = T_{c,tgs} = U, Service, nu, lt, K_{c,tgs}$$

Step 3: [TGS ⟶ C]. In response to the client request TGS replies with the session key($K_{c,tgs}$) and timestamp (nu) which is encrypted with (K_c).

$$TGS \rightarrow C: \{K_{c,tgs}, n\}K_c, \{T_{c,tgs}\}K_{tgs}$$

Step 4: In this step a authenticator (A_c) is generated

$$A_c = \{U, ts\}K_{c,tgs}$$

Step 5: [Client ⟶ TGS]. In this step authenticator, service

name, TGT and timestamp is sent to TGS.

$$C \rightarrow TGS: A_c, \{T_{c,tgs}\}K_{tgs}, S, nu$$

Step 6: In this step TGS verifies the authenticity of the client with the help of authenticator if client gets authenticated then it generates a service ticket ($T_{c,s}$or ($T_{service}$) which contains service name, username, timestamp, session key ($K_{c,s}$).

$$T_{c,s} = T_{service} = U, Service, nu, IPlist, lt, K_{c,s}$$

Step 7: [TGS→ Client]. In this step TGS sends the service ticket to the client with is encrypted with the shared secret key between application server and TGS.

$$TGS \rightarrow C: \{K_{c,s}, nu\}K_{c,tgs}, \{T_{c,s}\}K_s$$

Step 8: [Client→ Application Server]. In this both application server and client verifies the authenticity of each other as client provides the authenticator and service ticket to the application server.

$$C \rightarrow Server: \{A_c\}K_{c,s}, \{T_{c,s}\}K_s$$

Step 9: After authentication has been done the communication starts with messages encrypted with the shares secrete key ($K_{c,s}$).

VI. BAN LOGIC

BAN logic stand for M. Burrows, M. Abadi and R. Needham which is used for verifying the authenticity of messages for this it uses three main steps [12]:

1. Firstly proposed the assumptions for the protocol and represent them in symbolic form.
2. Check whether the assumptions made are fulfilling the goals or not.
3. Now apply the rules for acquiring the goal.

BAN *Logic* [13] *Constructs*:

$A| \equiv S: A\ believes\ S (i.e. may\ act\ as\ if\ S\ is\ true)$
$A \lhd X: A\ has\ received\ a\ message\ X.$
$A \sim X: A\ once\ said\ X, A\ sent\ a\ message\ X$
S
$\Rightarrow A: S\ has\ jurisdiction\ over\ A\ (S\ has\ authority\ on\ A)$
$\#(X): X\ is\ fresh$
$A \overset{k}{\leftrightarrow} B: K\ is\ a\ shared\ key\ between\ A\ and\ B$
$\{X\}k: Message\ X\ is\ encrypted\ by\ the\ key\ K$

BAN logic postulates:

Every Postulates of BAN logic have two parts: One is numerator (condition) and other is denominator (result).

Postulate 1: *Message Meaning Rules*

$$\frac{A| \equiv \ B \overset{K}{\leftrightarrow} A, A \lhd X}{A| \equiv B \sim X}$$

It means that A believes that the key K is shared with B only and any message X received at A if encrypted by K then it is sent by B only.

Postulate 2: *Part of Message Rules*

$$\frac{A| \equiv \#(X)}{A| \equiv \#(X, Y)}$$

This Postulates proves to A that if any message part is received recently by A then all the other parts of the message are received recently. It prevents replays confusion.

Postulate 3: *Nonce Verification Rules*

$$\frac{A| \equiv \#(X), A| \equiv B \sim X}{A| \equiv B| \equiv X}$$

It proves that A believes what B believes.

If A believes that X is recently sent by B, then A would believe that B believes X.

Postulate 4: *Jurisdiction Rule*

$$\frac{A| \equiv B| \equiv (X, Y), A| \equiv B \Rightarrow (X)}{A| \equiv X}$$

If A believes that B has jurisdiction over X, then A trusts B on the truth of X. A also believes that B believes message (x, y).

VII. PROBLEM

Kerberos has many advantages but there are always some issues and hence Kerberos also have some issues like KDC Quality of Services and one of the major issues on which research is going on is replay attack.

Replay attack

An issues in Kerberos protocol is Replay attack. It is a type of attack in which information is malignantly deferred and repeated by an intruder. It has numerous systems for making replay attack difficult like authenticators mostly depends upon machine's and clocks are synchronized, but sometimes synchronization protocols are note authenticated. In some cases, server is manipulated about the right time and hence attacker uses replay attack. Also, attacker can attack with in the session. Addition to that if we reduce the time then client can face some issues related to synchronization. Another method is use of cache, this cache can hold all authenticators that are allowed during session. In recent modification to Kerberos all the keys are stored in a shared memory but still this memory space can also be attacked. When TGS return a authenticator it is stored in an accessible space, hence can be attacked. Unix Systems cannot store authenticators in TCP based Model. So, replay attack can cause great amount of information loss as by using it one can get full excess of the service with someone else credentials. However, some researchers are suggesting the integrity protections which is not cost efficient.

VIII. SOLUTION

To address the problem defined about we have two modify the Kerberos authentication protocol in which we have introduced a new unique value i.e. MAC Address of user. As MAC Address uniquely identify an adapter so hence if we add it to our message it can help us in reducing the replay attack in Kerberos. Because intruder has to decrypt the MAC Address of the user which is time consuming and hence can prevent replay attack as it will cause time synchronization issue. For this we propose a database server which contains the legitimate users physical address and can be used to matched with the received MAC Address.

If the received MAC Address does not match then it can generate an error.

If the MAC Addresses does match then client and server can continue the communication and hence can get authenticated with reduced reply attacks.

Modified Kerberos Authentication Protocol using MAC:

$$1.\ A \rightarrow S: A, N_a, B$$

We added a new rule to BAN logic. This rule identify the client as authentication servers will verify the MAC Address which it received in the ticket.

Table1: Assumptions based on Logical believe

$S \mid = A \overset{K_{as}}{\leftrightarrow} S$
$A \mid = A \overset{K_{as}}{\leftrightarrow} S$
$B \mid = B \overset{K_{bs}}{\leftrightarrow} S$
$S \mid = B \overset{K_{bs}}{\leftrightarrow} S$
$S \mid = \#(N_a)$ $A \mid = \#(N_S)$
$B \mid = \#(N_a)$
$A \mid = \#(N_b)$
$B \mid = \#(N_S)$ $A \mid = S \ ?\ MAC_b$
$A \mid = S \ ?\ K_{ab}$
$S \mid = A \ ?\ MACa$
$S \mid = B \ ?\ MAC_b$
$A \mid = S \ ?\ MACa$
$B \mid = S \ ?\ K_{ab}$

BAN Modification:

$$\frac{B|\equiv S|\equiv (X,Y), B|\equiv S \Rightarrow (X,Y), B \lhd (X)_Y}{B|\equiv X, B|\equiv Y}$$

Jurisdiction rule is modified in a way that if X is present in ticket then it should be same as of X in X present in authenticator where X we supposed as MAC address of client. Also the X present in equation 2 has to match X present in equation 4 where we have supposed X as application server MAC address which is obtained from ARP table. When client requested the ticket from TGS in reply it gets ticket which contain authenticator and MAC address which is encrypted using a key called as session key.

Messages got by application server can be verified by decrypting authenticator using session key which will give us the two MAC Addresses and hence can be used as a proof of verification and hence will decrease the effect of replay attacks.

Our Proof:

BAN Logic should satisfy some conditions for secure connection and following are the conditions:

Time of generation of ticket i.e. Time stamp.

1. Encryption keys.
2. MAC addresses of client.

$$\frac{A|\equiv A \overset{K_{as}}{\leftrightarrow} S, A \lhd \{N_s, MAC_a, K_{ab}, B, \{N_S, MAC_a, K_{ab}, A\}K_{as}}{A|\equiv S \sim \{N_S, MAC_b, K_{ab}, B, \{N_S, MAC_a, K_{ab}, A\}K_{bs}\}K_{as}} \quad \text{---------- (1)}$$

$$\frac{A|\equiv \#(N_S)}{A|\equiv \#\{N_S, MAC_b, K_{ab}, B, \{N_S, MAC_a, K_{ab}, A\}K_{bs}\}K_{as}} \quad \text{---------- (2)}$$

$$\frac{(1),(2)}{A|\equiv S\ |\equiv \{N_S, MAC_b, K_{ab}, B, \{N_S, MAC_a, K_{ab}, A\}K_{bs}\}K_{as}} \quad \text{---------- (3)}$$

$$\frac{(3), A|\equiv S \Rightarrow (K_{ab}, MAC_b), A \lhd (MAC_b)K_{ab}}{A|\equiv K_{ab}} \quad \text{---------- (4)}$$

In equation 3, in order to use the authenticator client needs to believe session key, and for doing that it firstly should believes the ticket and following equations prove this:

$$\frac{B|\equiv \#(N_S)}{B|\equiv \#\{N_S, MAC_b, K_{ab}, A\}K_{bs}} \quad \text{---------- (5)}$$

$$\frac{B|\equiv B \overset{K_{bs}}{\leftrightarrow} S, A \lhd \{N_s, MAC_a, K_{ab}, A\}K_{bs}}{B|\equiv S \sim \{N_S, MAC_b, K_{ab}, A,\}K_{bs}} \quad \text{---------- (6)}$$

$$\frac{(5),(6)}{B|\equiv S\ |\equiv \{N_S, MAC_b, K_{ab}, A,\}K_{bs}} \quad \text{---------- (7)}$$

As per the new jurisdiction rule, that if clients MAC address from ARC table matches the MAC address present in the authenticator and also if client believes that server has sent the ticket (6) and client believes that server got jurisdiction of session key(k_{ab}) then we can call that B believes A.

$$\frac{(6), B|\equiv S \Rightarrow (K_{ab}, MAC_a), B \lhd (MAC_a)K_{ab}}{B|\equiv K_{ab}} \quad \text{---------- (8)}$$

As per the proofs we can see that the mac address i.e. also called as physical address can be used to prove the authentication of client to server and hence can reduced the replay attacks.

IX. Conclusion

We have explained the working of Kerberos in detail which will be very useful for the new uses of Kerberos.

After that we have modified the Kerberos for improving its working ability in presence of replay attacks and for that we have also modified BAN logics which proves that our modifications reduce the effect of replay attacks.

In the modifications we have purposed to add a physical address i.e. MAC address of client in the ticketing process to increase its robustness towards replay attacks.

We have also modified BAN logic to accommodate our changes (MAC Address) to its proofs.

In the final section we have proved using BAN Logic that our new Kerberos is more effective in reducing replay attacks.

References

1. B. C. Neuman, and T. Y T'so. "Kerberos: An Authentication Service for Computer Networks", IEEE Communications,1994, 32(9):33-38.
2. J. T. Kohl, B. C. Neumanand T. Y. T'so. "The Evolution of the Kerberos Authentication System". In Distributed Open Systems, IEEE Computer Society Press, 1994 pages 78-94.
3. T. Yu, S. Hartmanand K. Raeburn. "The Perils of Unauthenticated Encryption: Kerberos Version 4". In Proceedings of the Network and Distributed System Security Symposium. The Internet Society, 2004.
4. R. Bhandari and S. Sharma "Kerberos: Simplified Ticketing", IJARCSSE, 3(11), 2013,pp. 647-650.
5. http://web.mit.edu/kerberos/papers.html
6. http://kerberos.org/software/tutorial.html.
7. en.wikipedia.org/wiki/NT_LAN_Manager.
8. http://msdn.microsoft.com/en-us/library.
9. http://windowsitpro.com/security
10. M. Burrows, and M. Abadi, and R. Needham, "A logic ofauthentication". ACM Transactions on Computer Systems(TOCS), ACM New York, NY, USA, 1990, pp. 18-36.
11. Gong, L., Needham, R. and Yahalom, R., "Reasoning aboutbelief in cryptographic protocols", IEEE Symposium onSecurity and Privacy, 1999, pp. 234.
12. B. Kemal, and B. Nazife, "One-Time Passwords: Security Analysis Using BAN Logic and Integrating with Smartcard Authentication", Lecture notes in computer science, Springer, 2003, pp. 794-801.
13. Abdel Majid, N.T., Hossain M.A., Shepherd, S., Mahmoud, K. "Improved Kerberos Security Protocol Evaluation using Modified BAN Logic", IEEE Computer and Information Technology (CIT), 2010
14. R. Bhandari, S. Sharma, and N. Sharma, "Analysis of Windows Authentication Protocols: NTLM and Kerberos," in International Conf. on Computer Networks and Information Technology. Chandigarh, 2014, pp. 254-263.

AUTHORS PROFILE

Mr Randhir Bhandari is perusing Ph.D (CSE) course from the Department of Computer Science & Engineering, from Lovely Professional University, Jalandhar (INDIA). He has got his M.tech (CSE) from Shoolini University, Solan, Himachal Pradesh (INDIA), He has got his B.tech (CSE) from Himachal Pradesh University, Shimla, Himachal Pradesh (INDIA), He is Presently working as a Senior Faculty-IT at iNurture Education Solutions Pvt. Ltd, Banglore (INDIA) has ten year's of experience in the field of Computer Science and Engineering.

Mr. Digvijay Puri is perusing Ph.D (CSE) course from the Department of Computer Science & Engineering from Jaypee University of Information and Technology, Waknaghat, Solan, Himachal Pradesh(INDIA). He has got his M.tech (CSE) from Bahra University, Solan, Himachal Pradesh (INDIA), He has got his B.tech (IT) from Himachal Pradesh University, Shimla, Himachal Pradesh (INDIA) and He has got his Polytechnic (IT) from Punjab State Board of Technical University, Chandigarh, Punjab (INDIA). He is Presently working as a Senior Faculty-IT at iNurture Education Solutions Pvt. Ltd, Banglore (INDIA) has 5+ Year's of experience in the field of Computer Science and Engineering.

.

Ms. Natasha Sharma is perusing Mtech (CSE) course from the Department of Computer Science & Engineering from Himachal Pradesh University, Shimla, Himachal Pradesh(INDIA). She has got his B.tech (CSE) from from Himachal Pradesh University, Shimla, Himachal Pradesh (INDIA). She is Presently working as a Faculty-IT at iNurture Education Solutions Pvt. Ltd, Banglore (INDIA) has 2 Year's of experience in the field of Computer Science and Engineering.